МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. І. ВЕРНАДСЬКОГО

Кваліфікаційна наукова
праця на правах рукопису

СТУДЗІНСЬКИЙ РОМАН ВІКТОРОВИЧ

УДК 35-027.21:351.86](477)

ДИСЕРТАЦІЯ

РОЗВИТОК МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

281 «Публічне управління та адміністрування»

Подається на здобуття ступеня доктора філософії

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

_____Роман СТУДЗІНСЬКИЙ

Науковий керівник: Кучерявий Володимир Миколайович, доктор філософії з публічного управління та адміністрування, доцент

КИЇВ-2026

АНОТАЦІЯ

Студзінський Р.В. Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України. – На правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії за спеціальністю 281 – Публічне управління та адміністрування. Таврійський національний університет імені В. І. Вернадського. – Київ, 2026.

У дисертації вирішене актуальне наукове завдання, що полягає у теоретичному обґрунтуванні засад публічного управління у сфері забезпечення кібербезпеки та розробленні практичних рекомендацій щодо розвитку механізмів його реалізації в сучасних умовах.

У роботі запропоновано комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України, у контексті якого виділено три основні напрями, а саме: удосконалення *нормативно-правового забезпечення*, зокрема необхідно провести системну ревізію чинного законодавства; формування чіткої ієрархі нормативно-правових актів; законодавчо уточнити компетенції СБУ, ДССЗЗІ, НКЦК при РНБО, Нацполіції та Мінцифри; адаптувати законодавство до директив ЄС (NIS2), стандартів НАТО, ISO/IEC; запровадити механізм регулярного правового моніторингу; регулярно оновлювати законодавство у сфері застосування штучного інтелекту, хмарних сервісів, Big Data; розробити спеціальні норми щодо публічно-приватного партнерства у сфері кібербезпеки; визначити стимули для приватного сектору; удосконалення *організаційного забезпечення*, зокрема необхідно оптимізувати організаційну структуру системи кібербезпеки; удосконалити систему підготовки та перепідготовки кадрів; нарощувати ресурсний потенціал забезпечення кіберпідрозділів; запровадити єдину систему стратегічного та оперативного планування у сфері кібербезпеки; інституціоналізувати ризик-орієнтований підхід; сформувати регіональні координаційні механізми кібербезпеки та ін.; удосконалення *інформаційно-технічного забезпечення*, зокрема необхідно модернізувати

інформаційно-технічну інфраструктуру органів публічної влади; оновити програмно-апаратні комплекси; розробити та впровадити єдині технічні стандарти і протоколи інформаційної взаємодії; уніфікувати програмно-апаратні рішення; запровадити автоматизовані системи збору, аналізу та обробки даних про кіберінциденти; цифровізувати управлінські процеси; удосконалити інформаційно-аналітичні системи моніторингу кіберзагроз; впровадити технології аналізу великих даних і кореляції подій; посилити криптографічний та технічний захист інформації; удосконалити систему резервного копіювання та відновлення даних та ін.

Крім того, удосконалено теоретичне розуміння сутності поняття «публічне управління у сфері забезпечення кібербезпеки», під яким запропоновано розуміти цілеспрямовану, скоординовану та інноваційно орієнтовану діяльність, яка здійснюється органами державної влади, органами місцевого самоврядування та іншими суб'єктами публічної влади, на яку покладено завдання формувати, реалізовувати та оцінювати політики кіберзахисту, забезпечувати кіберстійкість держави, захист цифрового суверенітету, критичної інфраструктури й інформаційного простору, використовуючи нормативно-правові, організаційні, інформаційно-технологічні механізми у взаємодії з приватним сектором, громадянським суспільством та міжнародними інституціями.

Запропоновано напрями імплементації кращого зарубіжного досвіду у сфері публічного управління у сфері забезпечення кібербезпеки, зокрема: гармонізація нормативно-правового забезпечення, у контексті чого рекомендується привести у відповідність українські норми за зразком європейських стандартів (NIS2), з метою полегшення інтеграції до єдиного цифрового ринку; інституційний аспект, у контексті якого рекомендується створити єдиний національний координаційний центр з питань кібрбезпеки з міжвідомчим статусом (США); забезпечення безпечного електронного урядування, у контексті чого рекомендується впровадити єдину цифрову ідентифікацію громадян та захистити державні онлайн-сервіси; оптимізація

цифрової освіти, у контексті чого рекомендується масштабувати програми цифрової грамотності, внести теми кібербезпеки у навчальні курси кожного рівня освіти (країни Європейського Союзу); посилення міжнародної кооперації, у контексті чого рекомендується розширити участь в міжнародних кіберструктурах, здійснювати обмін інформацією, організовувати спільні тренування та круглі столи; посилення кадрової підготовки, у контексті чого рекомендується створити кіберрезерв, здійснювати підтримку IT-освіти та розвивати співпрацю держави, університетів і бізнесу (Ізраїль); забезпечення громадського контролю, у контексті чого рекомендується забезпечити прозорість державної політики, підвищити інклюзивність процесів і залучити громадянське суспільство до процесу забезпечення кібербезпеки.

Розроблено комплекс інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури, серед яких: системи виявлення загроз на основі штучного інтелекту та машинного навчання (AI/ML); платформи управління кіберінцидентами (SOAR, SIEM нового покоління); технології Zero Trust; хмарні та гібридні рішення кіберзахисту; автоматизовані системи резервного копіювання та відновлення (Disaster Recovery, Backup as a Service); кіберфізичні системи захисту промислових мереж (ICS/SCADA Security); технології блокчейн для забезпечення цілісності даних; кіберрозвідка, цифрові двійники та симуляційні платформи; VR/AR-тренінги з кібербезпеки.

Подальшого розвитку набуло бачення глобальних тенденцій та викликів у сфері забезпечення кібербезпеки, серед яких виділено: зростання кількості та складності кібератак, мілітаризація кіберпростору, діджиталізація критичної інфраструктури, поширення IoT та кіберфізичних систем, хмарна трансформація та ризики зберігання даних, недостатня цифрова грамотність населення, кадровий дефіцит кіберфахівців, політизація та фрагментація кіберпростору, зростання кіберзлочинності та тіньових кіберринків, виклики регулювання штучного інтелекту, проблеми захисту персональних даних, дезінформація та інформаційні операції.

Окреслено особливості управління ризиками кібербезпеки в умовах цифровізації публічного управління, серед яких: зростання цифрової залежності, ускладнення кіберзагроз, нерівномірність цифрової зрілості органів влади, інтеграція нових технологій, потреба в міжвідомчій координації, людський фактор як ключовий елемент ризику, необхідність динамічного управління ризиками, брак кадрів і компетенцій, підвищені вимоги до захисту персональних даних, необхідність комплексного, багаторівневого підходу.

Ключові слова: публічне управління, механізми публічного управління, цифрова трансформація, технологічний розвиток, кіберпростір, кібербезпека, забезпечення кібербезпеки, кібератаки, кіберзлочини, кіберзахист, кібероборона.

ANOTATION

Studzinsky R.V. Development of public administration mechanisms in the field of ensuring cybersecurity in Ukraine. – In the form of a manuscript.

Dissertation for the degree of Doctor of Philosophy in specialty 281 – Public Management and Administration. – V.I. Vernadsky Tavrichesky National University. Kyiv, 2026.

The dissertation solves a relevant scientific problem, which consists in the scientific and theoretical substantiation of the principles of public administration in the field of ensuring cybersecurity and the development of practical recommendations for the development of mechanisms for its implementation in modern conditions.

The work proposes a comprehensive mechanism for improving public administration in the field of ensuring cybersecurity in Ukraine, in the context of which three main areas are highlighted, namely: improving regulatory and legal support, in particular, it is necessary to conduct a systematic revision of current legislation; form a clear hierarchy of regulatory and legal acts; legislatively clarify the competencies of the SBU, DSSSII, NKCC under the NSDC, the National Police

and the Ministry of Digital Affairs; adapt the legislation to EU directives (NIS2), NATO standards, ISO/IEC; introduce a mechanism for regular legal monitoring; regularly update legislation in the field of application of artificial intelligence, cloud services, Big Data; develop special norms for public-private partnership in the field of cybersecurity; determine incentives for the private sector; improve organizational support, in particular, it is necessary to optimize the organizational structure of the cybersecurity system; improve the system of training and retraining of personnel; increase the resource potential of cyber units; introduce a unified system of strategic and operational planning in the field of cybersecurity; institutionalize a risk-oriented approach; form regional coordination mechanisms for cybersecurity, etc.; improve information and technical support, in particular, it is necessary to modernize the information and technical infrastructure of public authorities; update software and hardware complexes; develop and implement unified technical standards and protocols for information interaction; unify software and hardware solutions; introduce automated systems for collecting, analyzing and processing data on cyber incidents; digitize management processes; improve information and analytical systems for monitoring cyber threats; introduce technologies for analyzing big data and event correlation; strengthen cryptographic and technical protection of information; improve the data backup and recovery system, etc.

In addition, the theoretical understanding of the essence of the concept of "public governance in the field of cybersecurity" has been improved, under which it is proposed to understand purposeful, coordinated and innovation-oriented activities carried out by state authorities, local governments and other public authorities, which are tasked with forming, implementing and evaluating cyber security policies, ensuring the cyber resilience of the state, protecting digital sovereignty, critical infrastructure and information space, using regulatory, organizational, information and technological mechanisms in interaction with the private sector, civil society and international institutions.

Directions for implementing the best foreign experience in the field of public governance in the field of cybersecurity have been proposed, in particular:

harmonization of regulatory and legal support, in the context of which it is recommended to bring Ukrainian norms in line with European standards (NIS2), in order to facilitate integration into the single digital market; institutional aspect, in the context of which it is recommended to create a single national coordination center for cybersecurity with interdepartmental status (USA); ensuring secure e-government, in the context of which it is recommended to implement a single digital identification of citizens and protect state online services; optimizing digital education, in the context of which it is recommended to scale digital literacy programs, introduce cybersecurity topics into training courses at each level of education (European Union countries); strengthening international cooperation, in the context of which it is recommended to expand participation in international cyber structures, exchange information, organize joint training and round tables; strengthening personnel training, in the context of which it is recommended to create a cyber reserve, support IT education and develop cooperation between the state, universities and business (Israel); ensuring public control, in the context of which it is recommended to ensure transparency of state policy, increase the inclusiveness of processes and involve civil society in the process of ensuring cybersecurity.

A set of innovative cyber defense tools has been developed for critical infrastructure facilities, including: threat detection systems based on artificial intelligence and machine learning (AI/ML); cyber incident management platforms (SOAR, new generation SIEM); Zero Trust technologies; cloud and hybrid cyber defense solutions; automated backup and recovery systems (Disaster Recovery, Backup as a Service); cyber-physical systems for protecting industrial networks (ICS/SCADA Security); blockchain technologies to ensure data integrity; cyber intelligence, digital twins and simulation platforms; VR/AR cybersecurity training.

The vision of global trends and challenges in the field of cybersecurity has been further developed, including: the growth in the number and complexity of cyberattacks, the militarization of cyberspace, the digitalization of critical infrastructure, the spread of IoT and cyber-physical systems, cloud transformation and data storage risks, insufficient digital literacy of the population, a shortage of

cyber specialists, the politicization and fragmentation of cyberspace, the growth of cybercrime and shadow cyber markets, the challenges of regulating artificial intelligence, problems of personal data protection, disinformation and information operations.

The features of cybersecurity risk management in the context of digitalization of public administration are outlined, including: growing digital dependence, increasing complexity of cyber threats, uneven digital maturity of government agencies, integration of new technologies, the need for interagency coordination, the human factor as a key element of risk, the need for dynamic risk management, lack of personnel and competencies, increased requirements for personal data protection, the need for a comprehensive, multi-level approach.

Keywords: public administration, public administration mechanisms, digital transformation, technological development, cyberspace, cybersecurity, ensuring cybersecurity, cyberattacks, cybercrimes, cyberprotection, cyberdefense.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України (одноосібні):

1. Студзінський Р. В. Роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні. *Інвестиції: практика та досвід.* № 22. 2025. С. 355-358.
DOI: 10.32702/2306-6814.2025.22.355
URL: https://www.nayka.com.ua/index.php/investplan/article/view/8085/8217

2. Студзінський Р. В. Теоретичні основи публічного управління у сфері забезпечення кібербезпеки України. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* № 18. 2025.
DOI: https://doi.org/10.54929/2786-5746-2025-18-02-03
URL: https://reicst.com.ua/pmtl/article/view/2025-18-02-03/2025-18-02-03

3. Студзінський Р. В. Зарубіжний досвід управління у сфері забезпечення кібербезпеки та його імплементація в Україні. *Наукові інновації та передові технології.* № 1 (53). 2026. С. 270-280.

DOI: https://doi.org/10.52058/2786-5274-2026-1(53)-270-281
URL: https://perspectives.pp.ua/index.php/nauka/article/view/35574

Тези конференцій

4. Студзінський Р. В. Необхідність забезпечення кібербезпеки України в сучасних умовах. Матеріали IX міжнародної науково-практичної конференції «Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України» (м. Київ, 11 листопада 2025 р.) С. 36-38.

5. Студзінський Р. В. Наукові підходи до визначення публічного управління у сфері забезпечення кібербезпеки України. Матеріали Міжнародної науково-практичної конференції «Наука, освіта, економіка та суспільство: адаптація до викликів 21 століття». (Сан-Франциско, США, 6 грудня 2025 р.). С. 156-158.

6. Студзінський Р.В. Європейський досвід публічного управління у сфері забезпечення кібербезпеки. Матеріали LXIII Міжнародної науковопрактичної конференції «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (07 грудня 2025 р. м. Оломодць (Чехія). С. 60-62.

ЗМІСТ

ВСТУП 11

РОЗДІЛ 1 ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ 20

1.1. Глобальні тенденції та виклики у сфері забезпечення кібербезпеки 20

1.2. Сутність та зміст публічного управління у сфері забезпечення кібербезпеки 38

1.3. Цифровізація публічного управління як каталізатор розвитку кібербезпеки та ризик-менеджменту у цій сфері 57

Висновки до розділу 1 75

РОЗДІЛ 2 СУЧАСНИЙ СТАН РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ 78

2.1. Механізми публічного управління у сфері забезпечення кібербезпеки України 78

2.2. Особливості реалізації публічного управління у сфері забезпечення кібербезпеки України в умовах правового режиму воєнного стану 106

2.3. Проблеми реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України 126

Висновки до розділу 2 144

РОЗДІЛ 3 НАПРЯМИ ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ 1478

3.1. Зарубіжний досвід публічного управління у сфері забезпечення кібербезпеки 147

3.2. Шляхи удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України 166

3.3. Розвиток інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури 1890

Висновки до розділу 3 207

ВИСНОВКИ 210

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ 216

ДОДАТКИ 238

ВСТУП

Актуальність теми. Динамічний розвиток цифрових технологій, глобалізація інформаційних процесів і посилююча залежність суспільства та держави від інформаційно-комунікаційних систем спричиняють зростання значення кібербезпеки як головної складової національної безпеки. На тлі становлення цифрового суспільства кіберпростір трансформувався в стратегічно значущий сектор, де триває протистояння між державами, недержавними акторами й транснаціональними кіберугрупованнями, що обумовлює нові виклики для системи публічного управління.

Проблема гарантування кібербезпеки для України стала по-особливому актуальною через повномасштабну збройну агресію рф, що супроводжується постійними кібератаками на об’єкти критичної інфраструктури, органи державної влади, фінансову систему, мас-медіа й державні інформаційні ресурси. В нинішніх обставинах кіберзагрозам притаманна сисемність, яка поєднує технічні, інформаційно-психологічні й організаційно-управлінські впливи, що вимагає комплексної й скоординованої реакції зі сторони держави.

В той же час процеси цифровізації публічного управління, введення електронного урядування, зростання електронних публічних послуг та застосування хмарних технологій значно посилюють вимоги щодо результативності механізмів державного регулювання в секторі кібербезпеки. Недостатній рівень узгодженості нормативно-правового забезпечення, фрагментарність інституційної будови, обмеженість кадрових ресурсів і нерівномірність кіберзрілості органів публічної влади ослаблюють здатність держави відповідно протистояти новітнім кіберзагрозам.

В зазначених обставинах особливу роль відіграє наукове розуміння процесів розвитку механізмів публічного управління у сфері забезпечення кібербезпеки України, спрямоване на утворення цілісної, адаптивної і сталої системи управління кібербезпекою, що визначає покращення нормативно-правових, організаційних, інституційних, інформаційно-технічних та

кадрових механізмів, зважаючи на міжнародний досвід, стандарти ЄС і НАТО, і, крім того, своєрідність функціонування держави в обставинах воєнного стану.

Загальнометодологічні аспекти сфери публічного управління у сфері забезпечення кібербезпеки закладені у працях таких вчених як: С. Абрат, А. Алієв, Л. Арсенович, Н. Атаманова, І. Луняченко, О. Бакалінська, О. Бакалинський, Л. Веселова, І. Вівчар, А Вовк, Є. Вознюк, В. Андрюхіна, К. Герасимюк, Ю. Геращенко, О. Горун, В. Дзеньків, Г. Дзяна, Р. Дзяний, С. Дмитрів, С. Пікалюк, Є. Живило, Ю. Завгородня, Б. Конюхов, І. Костенко, В. Оксінь, Д. Левченко, В. Котух, К. Кочман, В. Крушеніцький, Є. Кубанов, В. Лазарів, Р. Лук'янчук, О. Мельник та інші. Водночас, актуальність зазначеної проблематики, її недостатня розробленість у вітчизняній науці публічного управління та нагальна потреба у практичних управлінських рішеннях зумовили вибір теми дисертаційного дослідження «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України».

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано в межах теми науково-дослідної роботи, що виконується кафедрою публічного управління, туризму та готельно-ресторанної справи Таврійського національного університету імені В. І. Вернадського «Трансформація механізмів публічного управління в умовах деокупації та реінтеграції Автономної Республіки Крим: глобалізаційний вимір» (номер державної реєстрації ДР № 0124U002260). Особистий внесок здобувача у виконання науково-дослідної роботи полягає у теоретичному обґрунтуванні шляхів удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України.

Мета і завдання дослідження. Метою дисертаційного дослідження є теоретичне обґрунтування засад публічного управління у сфері забезпечення кібербезпеки та розроблення практичних рекомендацій щодо розвитку

механізмів його реалізації в сучасних умовах. Досягнення поставленої мети передбачає вирішення відповідних *завдань*:

– охарактеризувати глобальні тенденції та виклики у сфері забезпечення кібербезпеки;

– розглянути сутність та зміст публічного управління у сфері забезпечення кібербезпеки;

– проаналізувати цифровізацію публічного управління як каталізатор розвитку кібербезпеки та ризик-менеджменту у цій сфері;

– здійснити аналіз механізмів публічного управління у сфері забезпечення кібербезпеки України;

– оцінити сучасний стан та проблеми реалізації публічного управління у сфері забезпечення кібербезпеки України;

– вивчити зарубіжний досвід публічного управління у сфері забезпечення кібербезпеки;

– запропонувати шляхи удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України;

– розробити напрями розвитку інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури.

Об’єкт дослідження – система публічного управління у сфері забезпечення кібербезпеки.

Предмет дослідження – розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України.

Методи дослідження. Теоретико-методологічною основою реалізації дослідницької мети слугує використання таких загальнонаукових і спеціальнонаукових методів, як: *аналізу та синтезу* – для деталізації об’єкта дослідження; *узагальнення* – для розкриття теоретико-методологічних засад публічного управління у сфері забезпечення кібербезпеки; *порівняльний метод та систематизації* – для вивчення нормативно-правового забезпечення публічного управління у сфері забезпечення кібербезпеки; *системний метод* – для розкриття концептуальних основ забезпечення

публічного управління у сфері забезпечення кібербезпеки; *логічний, діалектичний, метод узагальнення, комплексного і системного підходів* – для вдосконалення понятійного апарату дослідження; *статистичного аналізу, порівняння та узагальнення* – при дослідженні особливостей публічного управління у сфері забезпечення кібербезпеки; *метод прогнозування* – для виявлення можливих тенденцій розвитку публічного управління у сфері забезпечення кібербезпеки України; *графічний* – для наочного зображення отриманих статистичних розрахунків; *метод моделювання* – для розроблення напрямків удосконалення публічного управління у сфері забезпечення кібербезпеки України; *абстрактно-логічний метод* – для теоретичного узагальнення й формулювання висновків та пропозицій.

Методологічною базою дослідження є наукові праці вітчизняних і зарубіжних учених, зокрема, офіційні публікації міжнародних організацій. Інформаційну та емпіричну базу дослідження становили нормативні документи органів державної влади, статистичні та соціологічні дані, матеріали, опубліковані в періодичних виданнях та мережі Інтернет.

Наукова новизна одержаних результатів полягає в теоретичному обґрунтуванні засад публічного управління у сфері забезпечення кібербезпеки та розробленні практичних рекомендацій щодо розвитку механізмів його реалізації в сучасних умовах, що конкретизовано у таких наукових положеннях:

уперше:

– запропоновано комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України, у контексті якого виділено три основні напрями, а саме: удосконалення *нормативно-правового забезпечення*, зокрема необхідно провести системну ревізію чинного законодавства; сформувати чітку ієрархію нормативно-правових актів; законодавчо уточнити компетенції СБУ, ДССЗЗІ, НКЦК при РНБО, Нацполіції та Мінцифри; адаптувати законодавство до директив ЄС (NIS2), стандартів НАТО, ISO/IEC; запровадити механізм регулярного правового

моніторингу; регулярно оновлювати законодавство у сфері застосування штучного інтелекту, хмарних сервісів, Big Data; розробити спеціальні норми щодо публічно-приватного партнерства у сфері кібербезпеки; визначити стимули для приватного сектору; удосконалення *організаційного забезпечення*, зокрема необхідно оптимізувати організаційну структуру системи кібербезпеки; удосконалити систему підготовки та перепідготовки кадрів; нарощувати ресурсний потенціал забезпечення кіберпідрозділів; запровадити єдину систему стратегічного та оперативного планування у сфері кібербезпеки; інституціоналізувати ризик-орієнтований підхід; сформувати регіональні координаційні механізми кібербезпеки та ін.; удосконалення *інформаційно-технічного забезпечення*, зокрема необхідно модернізувати інформаційно-технічну інфраструктуру органів публічної влади; оновити програмно-апаратні комплекси; розробити та впровадити єдині технічні стандарти і протоколи інформаційної взаємодії; уніфікувати програмно-апаратні рішення; запровадити автоматизовані системи збору, аналізу та обробки даних про кіберінциденти; цифровізувати управлінські процеси; удосконалити інформаційно-аналітичні системи моніторингу кіберзагроз; впровадити технології аналізу великих даних і кореляції подій; посилити криптографічний та технічний захист інформації; удосконалити систему резервного копіювання та відновлення даних та інше;

удосконалено:

– теоретичне розуміння сутності поняття «публічне управління у сфері забезпечення кібербезпеки», під яким запропоновано розуміти цілеспрямовану, скоординовану та інноваційно орієнтовану діяльність, яка здійснюється органами державної влади, органами місцевого самоврядування та іншими суб’єктами публічної влади, на яку покладено завдання формувати, реалізовувати та оцінювати політики кіберзахисту, забезпечувати кіберстійкість держави, захист цифрового суверенітету, критичної інфраструктури й інформаційного простору, використовуючи нормативно-правові, організаційні, інформаційно-технологічні механізми у взаємодії з

приватним сектором, громадянським суспільством та міжнародними інституціями;

– напрями імплементації кращого зарубіжного досвіду у сфері публічного управління у сфері забезпечення кібербезпеки, зокрема: гармонізація нормативно-правового забезпечення, у контексті чого рекомендується привести у відповідність українські норми за зразком європейських стандартів (NIS2), з метою полегшення інтеграції до єдиного цифрового ринку; інституційний аспект, у контексті якого рекомендується створити єдиний національний координаційний центр з питань кібрбезпеки з міжвідомчим статусом (США); забезпечення безпечного електронного урядування, у контексті чого рекомендується впровадити єдину цифрову ідентифікацію громадян та захистити державні онлайн-сервіси; оптимізація цифрової освіти, у контексті чого рекомендується масштабувати програми цифрової грамотності, внести теми кібербезпеки у навчальні курси кожного рівня освіти (країни Європейського Союзу); посилення міжнародної кооперації, у контексті чого рекомендується розширити участь в міжнародних кіберструктурах, здійснювати обмін інформацією, організовувати спільні тренування та круглі столи; посилення кадрової підготовки, у контексті чого рекомендується створити кіберрезерв, здійснювати підтримку IT-освіти та розвивати співпрацю держави, університетів і бізнесу (Ізраїль); забезпечення громадського контролю, у контексті чого рекомендується забезпечити прозорість державної політики, підвищити інклюзивність процесів і залучити громадянське суспільство до процесу забезпечення кібербезпеки;

– комплекс інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури, серед яких: системи виявлення загроз на основі штучного інтелекту та машинного навчання (AI/ML); платформи управління кіберінцидентами (SOAR, SIEM нового покоління); технології Zero Trust; хмарні та гібридні рішення кіберзахисту; автоматизовані системи резервного копіювання та відновлення (Disaster Recovery, Backup as a Service); кіберфізичні системи захисту промислових мереж (ICS/SCADA Security);

технології блокчейн для забезпечення цілісності даних; кіберрозвідка, цифрові двійники та симуляційні платформи; VR/AR-тренінги з кібербезпеки;

набули подальшого розвитку:

– бачення глобальних тенденцій та викликів у сфері забезпечення кібербезпеки, серед яких виділено: зростання кількості та складності кібератак, мілітаризація кіберпростору, діджиталізація критичної інфраструктури, поширення IoT та кіберфізичних систем, хмарна трансформація та ризики зберігання даних, недостатня цифрова грамотність населення, кадровий дефіцит кіберфахівців, політизація та фрагментація кіберпростору, зростання кіберзлочинності та тіньових кіберринків, виклики регулювання штучного інтелекту, проблеми захисту персональних даних, дезінформація та інформаційні операції;

– особливості управління ризиками кібербезпеки в умовах цифровізації публічного управління, серед яких: зростання цифрової залежності, ускладнення кіберзагроз, нерівномірність цифрової зрілості органів влади, інтеграція нових технологій, потреба в міжвідомчій координації, людський фактор як ключовий елемент ризику, необхідність динамічного управління ризиками, брак кадрів і компетенцій, підвищені вимоги до захисту персональних даних, необхідність комплексного, багаторівневого підходу.

Практичне значення одержаних результатів полягає у можливості їх використання органами публічного управління під час формування і реалізації державної політики у сфері забезпечення кібербезпеки, зокрема при розробленні та удосконаленні нормативно-правових актів, стратегій, програм і концепцій цифрового розвитку та кіберзахисту. Результати дослідження можуть бути застосовані в діяльності центральних органів виконавчої влади, відповідальних за реалізацію політики кібербезпеки, для підвищення ефективності організаційних, інституційних та інформаційно-технічних механізмів публічного управління, удосконалення системи міжвідомчої координації та управління кіберризиками. Запропоновані напрями розвитку інноваційних інструментів кіберзахисту можуть бути використані суб’єктами

забезпечення кібербезпеки під час впровадження сучасних технологічних рішень, зокрема систем моніторингу кіберінцидентів, управління інформаційною безпекою, реагування на кібератаки та відновлення функціонування критично важливих систем.

Результати дисертації впроваджено в наукову діяльність та освітній процес Національної академії Служби безпеки України під час викладання навчальної дисципліни «Управління кіберінцидентами» (акт впровадження в освітній процес від 30.04.2026 р.); Національного технічного університету «Київський політехнічний інститут імені Ігоря Сікорського» під час проведення занять з освітнього компонента «Інформаційні технології в національній системі кібербезпеки України» (акт впровадження результатів дисертаційного дослідження від 12.03.2026 р.); Національної академії внутрішніх справ під час викладання навчальних дисциплін, підготовки навчально-методичних і дидактичних матеріалів (акт впровадження результатів дисертації від 10.04.2026 р. № 90-ОП); Таврійського національного університету імені В. І. Вернадського при формуванні змісту дисципліни «Глобалізація управління суспільними процесами, євроінтеграція та безпека» (довідка від 13.01.2026 р. № 18); Національної академії внутрішніх справ при підготовці монографій, підручників, навчальних посібників, методичних рекомендацій, обгрунтування пропозицій до чинних проектів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову (акт впровадження результатів дисертації від 10.04.2026 р. № 91-нд).

Особистий внесок здобувача. Наукові положення, висновки та практичні рекомендації, які характеризуються новизною і становлять цінність для розвитку науки публічного управління отримані автором самостійно.

Апробація результатів дослідження. Основні положення дисертаційного дослідження були презентовані та обговорені на міжнародних і всеукраїнських науково-практичних конференціях: IX міжнародній науково-практичній конференції «Теоретико-практичні засади управління, економіки

та природокористування: аспекти реінтеграції Криму в господарський комплекс України» (м. Київ, 11 листопада 2025 року), Міжнародній науково-практичній конференції «Наука, освіта, економіка та суспільство: адаптація до викликів 21 століття» (Сан-Франциско, США, 6 грудня 2025 р.) та LXIII Міжнародній науковопрактичній конференції «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (07 грудня 2025 року м. Оломодць (Чехія).

Публікації. Наукові результати дисертаційного дослідження опубліковано в 6 наукових працях, у тому числі в 3 статтях, опублікованих у фахових виданнях з публічного управління, віднесених до категорії «Б» та 3 тезах науково-практичних конференцій.

Структура дисертації. Дисертаційна робота складається із вступу, трьох розділів, висновків, списку використаних джерел. Її основний текст викладено на 215 сторінках, загальний обсяг становить 249 сторінок і включає 203 найменування використаних джерел.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

1.1. Глобальні тенденції та виклики у сфері забезпечення кібербезпеки

На тлі нинішньої динамічної цифрової трансформації питання забезпечення кібербезпеки стає пріоритетним як для держав, так і для міжнародних організацій, бізнесу й громадянського суспільства. Глобальні процеси інформатизації, зростання мережевих технологій, розповсюдження штучного інтелекту, Інтернету речей, хмарних сервісів та критично значущої інфраструктури утворюють нову цифрову реальність, де масштаби, структура й складність кіберзагроз інтенсивно збільшуються. Кіберпростір трансформувався у повноцінний геополітичний вимір, у якому між державами, транснаціональними корпораціями й злочинними угрупованнями відбуваються змагання за інформацію, ресурси й контроль критичних цифрових систем.

Зауважимо, що «кібербезпека стосується нових викликів у сфері безпеки, які торкаються як окремих організацій, так і суспільства загалом. Ці виклики зростають разом із цифровою трансформацією та збільшенням нашої залежності від взаємопов’язаних цифрових систем і послуг. Кібербезпека включає заходи, які компанії можуть застосовувати для захисту своїх важливих бізнес-систем, програмного забезпечення, пристроїв та мереж передачі даних від кіберзагроз. Ці загрози, що включають шкідливі події чи процеси, можуть серйозно вплинути на діяльність організації, її фінанси, дані та репутацію, а в гіршому випадку – і на безперервність її діяльності» [72]. Як зауважує Д. Попова, «заходи кібербезпеки, також відомі як кіберзахист, спрямовані на попередження атак, виявлення загроз та реагування на інциденти. Вони включають активні кроки для передбачення можливих атак і протидії потенційним кіберзагрозам. Це важливо, оскільки кіберзлочинці

часто мотивовані фінансовими, політичними або соціальними інтересами і використовують новітні технології для атак на критичну інфраструктуру, включаючи охорону здоров'я, фінансові установи та урядові організації» [113].

Погоджуємося з Г. Ортіною, що «інформаційна безпека є ключовим елементом національної безпеки будь-якої держави, особливо в умовах глобалізації, цифрової трансформації та посилення кіберзагроз. Сучасні виклики у сфері інформаційної безпеки зумовлені стрімким розвитком технологій, поширенням гібридних загроз, активізацією інформаційних воєн та кіберзлочинності. Відсутність ефективних механізмів протидії цим загрозам може призвести до критичних наслідків для державних інституцій, бізнесу та суспільства в цілому» [107]. Дійсно, глобальні тенденції розвитку кібербезпеки відзначаються одномоментним збільшенням можливостей і загроз технологічного характеру. Кардинальне зростання числа цифрових приладів, автоматизація рутинних процедур, введення кіберфізичних систем і штучного інтелекту обумовлюють актуальність потреби щодо нових підходів до захисту інформаційних ресурсів. Водночас триває зростання інструментів кіберзлочинності, зокрема від атак на критичну інфраструктуру до застосування нових методів соціальної інженерії, шкідливого програмного забезпечення, а також дезінформаційних операцій.

Як зазначає В. Горєлова, «кіберзлочинність має серйозні наслідки як для глобальної безпеки, так і для світової економіки. На глобальному рівні, кібератаки можуть спричиняти порушення функціонування державних інститутів, економічну дестабілізацію та загрози національній безпеці. Наприклад, кібератаки на електричні мережі, урядові структури або транспортні системи можуть паралізувати критичні елементи державної інфраструктури та створити хаос у суспільстві а економічні наслідки кіберзлочинності є надзвичайно великими. Так, згідно з оцінками, глобальні втрати від кіберзлочинності досягли трильйонів доларів, що включає не лише прямі фінансові збитки, але й витрати на відновлення після атак, компенсацію

постраждалим та заходи для забезпечення безпеки в майбутньому. Багато компаній витрачають значні ресурси на забезпечення кібербезпеки та відновлення своїх систем після атак, що знижує ефективність їхньої роботи та може призводити до втрати довіри споживачів. Відтак, кіберзлочинність є серйозним викликом для глобальної безпеки та економіки, і боротьба з цими загрозами вимагає ефективної міжнародної співпраці, зміцнення правових норм та розвитку нових технологій для протидії злочинності в цифровому середовищі» [26].

Головними викликами стають не тільки збільшення обсягу й складності кібератак, а також посилення асиметрії між ступенем кіберзахищеності держав; брак кваліфікованих спеціалістів; збільшення залежності соціуму від цифрових сервісів; і, крім того, постання нових правових, етичних, а також організаційних питань, що мають зв’язок із регулюванням кіберпростору. В таких обставинах глобальна кібербезпека стає багатоаспектною системою, яка охоплює чинники технологічного, правового, економічного, оборонного, дипломатичного та соціального характеру.

Дослідниця Г. Ортіна зауважує, що «одним із найсерйозніших викликів є масштабні кібератаки на державні установи та приватний сектор. Такі атаки, як правило, здійснюються через шкідливе програмне забезпечення, фішингові атаки та експлуатацію вразливостей у програмному забезпеченні. Особливої уваги потребують державні інформаційні системи, адже їхній злам може призвести до витоку конфіденційних даних або повного паралічу державного управління» [107]. Ще одним викликом є «інформаційні війни та маніпуляції громадською думкою. Використання фейкових новин, пропаганди та інформаційних маніпуляцій є невід’ємною складовою сучасних конфліктів. Соціальні мережі стали ефективним інструментом впливу на суспільну свідомість, і водночас платформою для розповсюдження дезінформації» [107]. До того ж, «особливу загрозу становить використання штучного інтелекту у сфері інформаційної безпеки. Штучний інтелект може бути використаний для розробки автоматизованих ботів, які поширюють фейки у соціальних мережах,

створення deepfake-відео, а також для здійснення складних кібератак із мінімальним втручанням людини. Це вимагає розробки нових методів виявлення та протидії таким загрозам» [107].

Ще одним з головних викликів, які постають перед сучасним глобальним суспільством на тлі цифрових загроз, є «забезпечення захисту прав людини в кіберпросторі. Кібербезпека, з одного боку, є необхідною для захисту від злочинних дій, таких як крадіжка особистих даних,шахрайство, кібератаки на критичні інфраструктури, а з іншого – вимагає дотримання фундаментальних прав і свобод, таких як право на приватність, свободу слова та право на доступ до інформації. У контексті цифрових загроз важливо підтримувати баланс між забезпеченням безпеки та захистом прав людини. Наприклад, застосування засобів кібербезпеки, таких як моніторинг інтернет активності громадян для виявлення потенційних кіберзлочинців, не повинно порушувати права на конфіденційність та особисту недоторканність. Використання новітніх технологій для виявлення кіберзлочинів повинно здійснюватися з дотриманням етичних принципів,що враховують потребу в захисті базових прав людини в цифровому середовищі» [26]. При цьому, «однією з найскладніших етичних дилему сфері кібербезпеки є питання балансу між конфіденційністю особистих даних і необхідністю боротьби з кіберзлочинами. Боротьба з кіберзлочинністю вимагає використання потужних технологій для моніторингу та аналізу великих обсягів інформації, однак це може призводити до порушень права на приватність. З одного боку, ефективне виявлення та попередження кіберзлочинів, таких як фінансові шахрайства чи кібертероризм, потребує доступу до великої кількості особистих даних. З іншого боку, ці дії можуть призвести до ненавмисного вторгнення в особисте життя громадян і порушення їхніх прав на конфіденційність. Тому важливо розробляти правові норми, які дозволяють забезпечити ефективний захист від кіберзлочинців, не порушуючи при цьому прав громадян на приватність» [26].

Група науковців П. Рогов, Б. Ворович та В. Ткаченко також зазначають, що «критична інфраструктура, яка забезпечує ключові функції держави та

суспільства, все більше піддається загрозам у цифровому просторі. Це пов'язано із зростаючою залежністю від інформаційних технологій і підключених до Інтернету систем, які керують різними процесами. Кіберзагрози стають серйозним викликом для захисту енергетичних мереж, транспорту, фінансових систем та телекомунікацій» [138]. Найбільш розповсюджені загрози – цифрові атаки, вразливість промислових систем управління і, крім того, кібератаки вітчизняних і міжнародних злочинних організацій.

А. Андрух зазначає, що «одним із найсерйозніших викликів для критичної інфраструктури держави є кібератаки на енергетичні системи. Електромережі,газопроводи,нафтопереробні заводи та інші енергетичні об'єкти є важливими цілями для хакерів. Збій у роботі таких систем може призвести до відключення електроенергії на великій території, паралізуючи інші сектори інфраструктури, включаючи транспорт, комунікації та фінанси. Транспортна інфраструктура також є важливою мішенню. Це стосується як громадського транспорту, так і міжнародних перевезень. Кібератаки на системи керування залізницями, авіацією чи морськими портами можуть спричинити величезні збої в логістиці, переривання транспортних ланцюжків і навіть потенційно створити загрози для життя людей. Фінансові системи, які є хребтом світової економіки, також піддаються постійним кібератакам. Зловмисники можуть атакувати банки, біржі, платіжні системи з метою викрадення грошей, знищення даних або проведення маніпуляцій на фінансових ринках. Телекомунікаційні системи, що забезпечують зв'язок між різними секторами критичної інфраструктури, також знаходяться під загрозою. Атаки на ці системи можуть призвести до відключення зв'язку, порушення роботи Інтернету або навіть використання мереж для шпигунства і збору інформації» [4]. Насамперед вразливими вважаються мобільні й широкосмугові мережі, які застосовують старі протоколи безпеки чи містять вразливості у їхній будові.

Варто також звернути увагу, що «використання технологій стеження для боротьби з кіберзлочинністю, таких як системи моніторингу онлайн-активності, аналізування даних користувачів чи впровадження систем масового стеження, може призвести до значних етичних і правових проблем. Хоча ці технології можуть допомогти у виявленні та запобіганні кіберзлочинам, вони також створюють ризик виникнення явища, яке часто називають «великою братом» – постійного нагляду за громадянами державою чи іншими суб'єктами. Ці технології можуть бути використані для моніторингу особистої діяльності громадян у мережі, що викликає побоювання щодо зловживань та порушень основоположних прав людини. Постійне стеження може спричинити втрату приватності, обмеження свободи вираження думок і навіть використовуватись для політичних чи соціальних репресій. Етичні аспекти такого стеження полягають у питаннях, наскільки далеко можна йти в обмеженні прав людини заради забезпечення національної безпеки чи боротьби з кіберзлочинністю. Тому важливо, щоб використання технологій стеження мало чіткі обмеження, контролювалося відповідними інститутами та не призводило до серйозних порушень основних прав і свобод людини. Тобто, етичні та правові аспекти кібербезпеки полягають у необхідності забезпечення захисту від кіберзлочинності без шкоди для прав людини, що потребує створення чіткої правової бази, яка балансуватиме між безпекою та особистими свободами» [26]. Отже, один з головних чинників міжнародного співробітництва щодо боротьби з кіберзлочинністю – потреба формування єдиних стандартів реагування на кібератаки. В кіберзлочинності не існує національних кордонів, через що стає більш складною боротьба з нею на рівні певних держав. Через це саме міжнародна співпраця вважається дуже важливою для результативного розв'язання проблеми.

До того ж, «розвиток Інтернету речей (IoT) відкриває нові можливості для автоматизації та покращення управління державною критичною інфраструктурою, але разом з тим створює нові вразливості. Із збільшенням кількості пристроїв, підключених до мережі, зростає і площа для потенційних

атак. Багато пристроїв IoT мають слабкі системи безпеки або використовують стандартні налаштування безпеки, що робить їх вразливими для кіберзлочинців. IoT пристрої, такі як датчики в енергетичних системах, камери відеоспостереження, розумні лічильники та інші, можуть стати мішенню для хакерів. Якщо ці пристрої будуть скомпрометовані, зловмисники можуть отримати доступ до ключових систем управління інфраструктурою або навіть організувати розподілені атаки на відмову в обслуговуванні (DDoS)» [4]. Також велика кількість приладів IoT застосовуються, щоб збирати інформацію, що теж спричиняє загрози витоку інформації. Це передусім є критичним у ситуаціях, коли йдеться про медичне устаткування, транспортні системи чи фінансові служби, де компрометація конфіденційної інформації може містити серйозні наслідки.

Як зазначають науковці, «у сучасному світі боротьба з кіберзлочинністю стає дедалі більш складною через швидкий розвиток технологій, які використовуються не лише для забезпечення безпеки,а й для здійснення злочинних дій. Важливою складовою цієї боротьби є застосування новітніх технологій, таких як штучний інтелект та аналітика великих даних, що мають значний потенціал у сфері кіберзахисту. З одного боку, ці технології можуть забезпечити своєчасне виявлення та нейтралізацію кіберзагроз, а з іншого – породжують низку етичних, правових і технічних проблем, які потребують ретельного аналізу та регулювання. Так, штучний інтелект і великі дані використовуються для аналізу величезних обсягів інформації, що надходить із різних джерел,зокрема з кіберпростору, в реальному часі. Це дозволяє виявляти аномалії, які можуть свідчити про спроби здійснення кіберзлочинів, таких як фішинг, зломи чи шкідливі програми. Штучний інтелект може допомогти в автоматизації процесів виявлення та реагування на кіберзагрози, що істотно знижує час на реакцію та зменшує ризик успіху атаки. Великі дані, в свою чергу, забезпечують можливість здійснювати комплексний аналіз та прогнозувати потенційні загрози, що дозволяє будувати більш ефективні стратегії кіберзахисту» [26]. Проте, «використання цих технологій несе з

собою не тільки переваги, але й суттєві ризики. Одним із головних ризиків є проблема захисту приватності особистих даних. Штучний інтелект і великі дані здатні збирати та обробляти великі обсяги персональної інформації, що ставить під загрозу конфіденційність. За допомогою таких технологій можна не лише захистити дані, а й порушити основні права людини, зокрема право на приватність та свободу особистої інформації. З цієї точки зору, етичні питання стають надзвичайно важливими,оскільки застосування штучного інтелекту в контексті кібербезпеки повинно забезпечувати баланс між захистом інтересів держави та правами людини» [190].

В. Дяченко та Н. Дяченко вважають, що з-поміж головних глобальних тенденцій забезпечення кібербезпеки в секторі інформаційних комунікацій доречно виділити:

– «постійно зростаючу кількість та складність кібератак, що обумовлює потребу безперервного оновлення систем захисту та підвищення кваліфікації персоналу;

– розширення периметра захисту через комунікації, що відбуваються поза межами офісних мереж;

– людський чинник, оскільки соціальна інженерія є ефективним інструментом для кіберзлочинців, які використовують довіру та необережність користувачів;

– динамічні зміни регуляторного середовища та необхідність забезпечити відповідність стандартам обумовлені потребою врегулювання законодавства у сфері захисту даних та кібербезпеки, зокрема, GDPR, HIPAA, національні стандарти;

– дефіцит кваліфікованих фахівців з кібербезпеки обумовлений стрімким розвитком технологій та зростанням загроз, що ускладнює набір та утримання кваліфікованого персоналу, який може ефективно протистояти сучасним кіберзагрозам;

– інтеграцію та сумісність систем безпеки, оскільки недостатня інтеграція може створювати «сліпі зони» та вразливості, через які можуть проникати зловмисники;

– потребу забезпечення неперервності бізнес-процесів, яка передбачає не лише необхідність формування кібербезпеки шляхом запобігання атакам, а й розробку планів відновлення після інцидентів та забезпечення неперервності бізнесу;

– фінансові та ресурсні обмеження, оскільки не всі організації мають достатні фінансові, економічні, інформаційні, технологічні та людські ресурси для впровадження комплексних рішень з кібербезпеки, що особливо актуально для малого та середнього бізнесу, який також може стати мішенню кіберзлочинців» [47].

Водночас потрібно зважати на ключові аспекти, які супроводжують механізми утворення кібербезпеки інформаційних комунікацій, з-поміж котрих:

– «зростання обсягів даних і складності інформаційних систем підвищують вразливість до кібератак;

– поширення нових технологій (IoT, 5G, хмарні обчислення) створюють додаткові можливості для зловмисників;

– соціальна інженерія та фішинг залишаються основними загрозами з урахуванням людського чинника» [47].

Вивчаючи питання тенденцій у сфері глобальної кібербезпеки, варто зважати на те, що вона – невід'ємна складова інформаційних технологій. В нинішніх реаліях динамічний розвиток і розповсюдження нових інформаційних та телекомунікаційних технологій формують передумови для глобальної інформаційної революції. Згаданий процес безпосередньо впливає на всі чинники функціонування держави, в тому числі на політику, економіку, управління, фінанси, культуру, науку й зростання інформаційних відносин.

В нинішніх обставинах зростання чисельності гібридних мереж під час утворення кібернетичної безпеки процесів інформаційних комунікацій

потрібна зважати на те, що:

– «поєднання хмарних, локальних та гібридних систем ускладнює захист інформаційних потоків;

– використання SD-WAN та VPN формує передумови безпечної передачі даних у гібридних середовищах;

– процеси формування захисту інформаційних потоків обумовлюють н

е Варто звернути увагу на те, що «у сучасному світі економіка активно в

провадж

ує п'яте покоління технологічних укладів, що базується на розвитку т

ехнологій для взаємодії між людиною та машиною через застосування ш

тучного інтелекту та машинного навчання. Передбачається, що в недалекому м

айбутньому основою для взаємодії учасників економічних процесів стане цифровий обмін даними. Це сприятиме розвитку нейромереж і подальшому в

досконаленню систем на базі штучного інтелекту. За оцінками міжнародних д

ослідників, штучний інтелект стає ключовим елементом цифрової т

рансформації, який відіграє важливу роль у переході економіки до нового р

івня взаємодії між людиною та машиною» [193]. Це, своєю чергою, допомагає з

ростанню цифрових платформ та загальному розвитку цифрової економіки.

Зокрема, «з використанням цифрових технологій, компанії, які належать до Індустрії 5.0, мають змогу значно підвищити свою продуктивність та ефективність. Технології, такі як автоматизація, аналіз даних та штучний інтелект, дозволяють оптимізувати процеси, зменшити витрати та підвищити т

агальну продуктивність. Цифрова трансформація також сприяє адаптації к

омпаній до змін у ринкових умовах, змінних вимогах споживачів та швидкому р

озвитку технологій. Одним з основних викликів є інтеграція сучасних т

ехнологій з застарілими системами, що може становити загрозу для безпеки і

та цілісності даних» [113]. Управління інформацією і кібербезпека вважаються к

ритично значущими складовими під час цифрової трансформації, насамперед з

важаючи на зростаючу залежність від рішень, ухвалених, базуючись на інформації, і застосування штучного інтелекту та машинного навчання, що а

н

о

потребує строгої відповідності щодо стандартів конфіденційності й безпеки інформації.

Забезпеченню кібербезпеки в часи розвитку Індустрії 5.0 властиві власні унікальні характерні ознаки, які спричинені змінами у технологічному розвитку, впровадженням штучного інтелекту, співдією людей та машин і, крім того, зростаючою залежністю від цифрових технологій у всіх секторах життя. Індустрія 5.0 акцентує не тільки на автоматизації, а також тісному співрбітництві між людьми й технологіями, що ставить вимогу стосовно нових підходів до кібербезпеки.

Важливо враховувати той факт, що «кібербезпека в рамках Індустрії 5.0 розкривається на декількох важливих рівнях, кожен з яких має свої специфіки та вимоги. На фізичному рівні безпека забезпечується через захист пристроїв інтернету речей, таких як датчики, часто встановлені в місцях, недоступних для постійного контролю. Захист цих пристроїв може включати в себе як прості рішення – наприклад, замкнені шафи для устаткування – так і більш складні, як системи сигналізації на панелі управління, що сповіщають про несанкціоновані спроби доступу, або системи відеоспостереження з функцією розпізнавання осіб. Людський фактор становить другий рівень кібербезпеки. Він акцентує на вразливості, що виникає через недостатню обізнаність або увагу працівників. Хакери часто використовують методи соціальної інженерії для отримання конфіденційної інформації від співробітників, підрядників та замовників, використовуючи їх некомпетентність як засіб доступу до корпоративних мереж. Третій рівень – організаційний, який раніше характеризувався розділенням обов'язків між різними командами, не завжди включаючи ІТ-безпеку в обов'язки кожної з них. Сучасні підходи вимагають інтегрованого захисту, який об'єднує кібербезпеку, забезпечення надійності систем та фізичний захист. Четвертий рівень кібербезпеки – технолгічний, має свої особливості. З одного боку, інтелектуальніші технології сприяють стримуванню, запобіганню та виявленню кібератак» [69]. Однак, з іншої сторони, кіберзагрози теж стають більш складними й розвиненими. Це

значить, що старі технологічні системи, котрі до цього визнавалися надійними й безпечними, наразі можуть бути вразливими місцями, через котрі хакери мають змогу одержати доступ до критично важливої інформації.

В Індустрії 5.0 забезпечення кібербезпеки припиняє бути тільки технічним завданням; вона потребує ґрунтовного осмислення взаємозв'язків між технологічними, процесуальними й людськими факторами. Ідентифікація ризиків та управління кібербезпекою стають більш складними, зважаючи на зростаючу коннектованість й автоматизацію, які притаманні Індустрії 5.0. Через це захист інфраструктури, контролювання доступу й навчання працівників мають стати пристосованими до нового сьогодення, в якому кіберзагрози стають дедалі складнішими й більш різноплановими.

У розрізі динамічного зростання Індустрії 5.0, коли провідні технології і штучний інтелект дедалі більше впроваджуються в усі сектори діяльності, питання кібербезпеки стають по-особливому актуальними. Зазначена нова епоха технологічних інновацій спричиняє як ряд нових викликів, так і забезпечує багато можливостей для гарантування безпеки власних систем та інформації. Здійснимо більш детальний розгляд того, яким чином розвиток кіберпростору в розрізі Індустрії 5.0 чинить вплив на зміну парадигми кібербезпеки, визначимо головні виклики й змоги (табл. 1.1).

Згадані виклики й змоги – значущі чинники для взяття до уваги під час напрацювання стратегій кібербезпеки в епоху Індустрії 5.0, даючи можливість не тільки відповідати на нові виклики, а також застосовувати нові змоги для поліпшення власної кіберстійкості.

Утворення глобального порядку кібербезпеки стає особливо актуальним, зважаючи на грунтовні трансформації, які здійснюються в секторі міжнародної безпеки, політики і технологій. В умовах динамічної цифровізації публічного управління, економіки, оборони й приватного сектора, питання розробки та введення єдиних глобальних норм, стандартів та процедур реагування на кіберзагрози являється необхідним підгрунтям стабільності та довіри в міжнародній спільноті. За висловлюванням В. Гавриляка, що

«європейська кібербезпекова стратегія, зокрема в рамках «Цифрового десятиліття», розглядає питання створення глобального / відкритого, стабільного та безпечного кіберпростору як ключового напряму розвитку безпекової політики ЄС. Це передбачає розбудову національних кіберспроможностей, інтеграцію стандартів у союзні системи, створення спільних інституцій типу Спільного кіберпідрозділу (Joint Cyber Unit), а також реалізацію принципу «кібербезпека за замовчуванням» у цифрових інфраструктурах» [21].

Таблиця 1.1

Ключові виклики та можливості в контексті кібербезпеки в епоху Індустрії 5.0

№ з/п	Виклики	Можливості
	Збільшення взаємозв'язків систем. Індустрія 5.0 характеризується розширеною інтеграцією цифрових технологій, що створює складніші мережі та збільшує потенційні вектори атак	Розумні системи виявлення загроз. Розвиток технологій дозволяє створювати більш розвинуті системи моніторингу і виявлення, які можуть передбачати і нейтралізувати загрози до того, як вони спричинять шкоду
	Автоматизація та автономні системи. Посилення використання автономних роботів і систем управління, керованих штучним інтелектом, вносить додаткові ризики, пов'язані з ненавмисними помилками в програмному забезпеченні та можливими зловмисними маніпуляціями	Захист інтеграції з блокчейн-технологіями. Блокчейн може забезпечити вищий рівень захисту даних через децентралізовану та незмінну структуру записів
	Загрози штучного інтелекту. Інтелектуальні системи можуть бути вразливими до атак з використанням даних, що вводяться (data що може призвести до некоректного прийняття рішень	Штучний інтелект у кібербезпеці. AI може бути використаний для автоматизації складних процесів виявлення і реагування на кіберзагрози, значно підвищуючи ефективність кібероборони
	Кіберфізичні системи та IoT. Широке впровадження кіберфізичних систем та інтернету речей створює великі виклики для забезпечення конфіденційності, цілісності та доступності критично важливих даних	Адаптивні системи безпеки. Розвиток технологій дозволяє створювати системи безпеки, які можуть адаптуватися до змін у загрозах в реальному часі
	Комплексність даних та їх захист. Ріст обсягів даних, їх різноманітність і швидкість обробки потребують вдосконалення методів захисту і зберігання	Освіта та навчання. Підвищення обізнаності та кваліфікації працівників у галузі кібербезпеки може значно знизити людські помилки і підвищити загальний рівень захищеності

Джерело: за матеріалами [113]

До того ж, зауважимо, в глобальному контексті перспективи утворення алгоритму кібербезпеки залежать від того, чи спроможні держави досягти консенсусу стосовно головних принципів кіберповедінки, а саме суверенітету в кіберпросторі, недопуску агресивного застосування кіберінструментів, прозорості діяльності, взаємної відповідальності за кібератаки і, крім того, взаємного визнання випадків кібертероризму. Така правова сфера повинна основуватися на міжнародному праві, в тому числі на принципах ООН стосовно поведінки держав у кіберпросторі. Як зазначено в дослідженні О. Семененка, «центральними викликами для глобального режиму є не лише технічна складність реагування на транскордонні атаки, а й брак узгоджених механізмів ідентифікації винних акторів, що унеможливлює оперативне введення санкцій або відповідних заходів без шкоди для міждержавної співпраці. Спроби створити глобальний режим кібербезпеки стикаються з системною конкуренцією між моделями цифрового суверенітету» [18]. Однак «створення функціонального глобального режиму кібербезпеки можливе за умови послідовної інтеграції регіональних ініціатив, таких як Стратегія кібербезпеки ЄС, зусиль ООН та спеціалізованих агенцій, як-от ITU. Ключову роль тут відіграватиме впровадження спільних механізмів сертифікації кіберзахисту, обміну вкрай важливою інформацією між національними CSIRT / CERT структурами, розвиток систем раннього попередженнята створення міжнародних груп швидкого реагування» [137].

Таким чином, перспективи утворення глобального режиму кібербезпеки мають зв’язок із введенням гнучкої моделі багатоступеневої взаємодії, що передбачає технічне, правове, організаційне й політичне об’єднання зусиль головних міжнародних акторів. Успішність зазначеної моделі залежить від формування механізмів довіри, підтвердження відповідальності за атаки й напрацювання єдиних нормативних умов, які прийнятні для переважного числа цифрових держав світу.

Насамкінець, згрупуємо виявлені глобальні тенденції та виклики у сфері забезпечення кібербезпеки у табл. 1.2.

Таблиця 1.2

Глобальні тенденції та виклики у сфері забезпечення кібербезпеки

Тенденція	**Характеристика**	**Для яких груп країн характерно**
1. Зростання кількості та складності кібератак	Зростання атак на державні органи, фінансову сферу, енергетику; використання складних багатоступеневих шкідливих програм, APT-кампаній	Розвинені країни (США, ЄС, Південна Корея, Японія); країни, що ведуть війну або перебувають під гібридним тиском (Україна)
2. Мілітаризація кіберпростору	Застосування кібератак як складової воєнних дій; організація кіберкоманд в збройних силах; зростання кіберзброї	Великі держави з потужним військовим та технічним потенціалом (США, Китай, РФ, Великобританія, Ізраїль)
3. Діджиталізація критичної інфраструктури	Збільшення залежності енергетичних систем, транспорту, водопостачання, медицини від цифрових платформ; зростання ризику системних збоїв	Усі країни, але найбільше — розвинені та країни з активною цифровізацією (ЄС, США, Сінгапур, Україна)
4. Поширення IoT та кіберфізичних систем	Зростання числа вразливих приладів, неіснування стандартів безпеки, застосування ботнетів	Глобально, особливо країни з високою проникністю Інтернету та «розумних» пристроїв (ЄС, США, Південна Корея)
5. Хмарна трансформація та ризики зберігання даних	Перехід на хмарні сервіси покращує результативність, проте обумовлює нові вразливості; ризики витоку й втрати інформації	Розвинені країни та країни, що активно модернізують держуправління (Канада, Україна, країни ЄС)
6. Недостатня цифрова грамотність населення	Розповсюдження фішингу, соціальної інженерії, контенту маніпулятивного характеру; малий рівень практичних навичок кіберзахисту	Країни, що розвиваються; пострадянський простір; регіони з низьким рівнем цифрової культури
7. Кадровий дефіцит кіберфахівців	Міжнародний дефіцит аналітиків, інженерів, офіцерів кібербезпеки; конкуренція держав та корпорацій	Глобально, але найбільше — у країнах із швидкою цифровізацією та малими ринками праці (Україна, країни Балтії, Скандинавія)
8. Політизація та фрагментація кіберпростору	Розрив між моделями регулювання (американська, китайська, європейська); збільшення цифрових перепон	Великі геополітичні блоки (США–ЄС–Китай); країни, які інтегруються в ці цифрові системи

9. Зростання кіберзлочинності та тіньових кіберринків	Зростання підпільних платформ, ринку інормації, RaaS (ransomware as a service)	Країни із слабким контролем правоохоронних органів; держави, де активно діють хакерські угруповання (РФ, Північна Корея)
10. Виклики регулювання штучного інтелекту	Використання штучного інтелекту з метою кібератак, маніпуляцій, генерації шкідливого контенту; потреба етичних і правових процедур контролювання	Розвинені країни, що розробляють нормативні акти (ЄС, США, Канада), а також країни, які впроваджують ШІ у держсектор
11. Проблеми захисту персональних даних	Масовий витік інформації, незаконний доступ до даних, застосування глобальних масивів з метою маніпуляцій	Усі групи країн, але найбільше — у державах із великими базами даних та е-сервісами (ЄС, США, Україна)
12. Дезінформація та інформаційні операції	Застосування цифрових платформ, щоб впливати на думку громадськості, вибори, політичні процеси	Країни з демократичними інститутами (ЄС, США), а також держави, що є об’єктом гібридних нападів (Україна)

Джерело: власна розробка автора

Здійснивши аналіз поданої інформації, можливо стверджувати, що новітнім глобальним тенденціям у сфері кібербезпеки властиві комплексність, багаторівневість й асиметричність, виражаючи нерівномірність цифрового зростання різних груп держав і своєрідність їх політичних, економічних та технологічних змог.

По-перше, найінтенсивніше збільшуються загрози, пов’язані зі збільшенням масштабів і складності кібератак. Високотехнологічні країни, такі як Сполучені Штати Америки, держави Євросоюзу, Японія, Південна Корея, найбільше страждають від складних APT-кампаній, а також атак на критичну інфраструктуру, що спричинено значним ступенем діджиталізації їх економік і великим обсягом стратегічно важливих цифрових ресурсів. По-особливому вразливими вважаються держави, які знаходяться в стані збройного конфлікту чи гібридної агресії, в тому числі Україна, на котру націлюються постійні та політично мотивовані кібератаки.

Друга важлива тенденція – мілітаризація кіберпростору, яка притаманна в основному великим державам, що мають потужні оборонно-технологічні комплекси. Все частіше кіберзасоби використовуються як доповнення до

традиційних військових операцій, а держави активно організовують кіберкомандування і вкладають інвестиції в кіберзброю. Згадана процедура збільшує глобальну нестабільність і формує новий вимір міжнародної конкуренції.

Водночас швидке зростання цифрової інфраструктури, перехід до хмарних сервісів і масове застосування IoT-пристроїв утворюють додаткові ризики для держав різних груп. Перед розвиненими державами постають виклики гарантування постійності функціонування складних технологічних систем, в той час, коли держави, які розвиваються, стикаються з браком стандартів, слабкою нормативно-правовою основою і неналежним фінансуванням кібербезпекових заходів.

Особливий інтерес викликає кадровий дефіцит, що вважається глобальною проблемою, проте найбільше виявляється в державах з інтенсивним зростанням цифрової економіки й недостатньою чисельністю кваліфікованих спеціалістів, як-от Україна, держави Балтії або Скандинавії. Брак професіоналів гальмує втілення державних стратегій кіберзахисту й, крім того, зменшує спроможність реагування на сучасні загрози.

Крім того, важливим трендом продовжує залишатися фрагментація кіберпростору, що виражається у різних моделях регулювання, від європейської, спрямованої на захист прав людини й інформації, до китайської, яка заснована на централізованому контролі, що обумовлює ризики цифрової нерівності, здійснює обмеження транскордонної взаємодії й збільшує технологічну конкуренцію між головними геополітичними блоками.

Державам, що мають слабкі інститути й обмежені ресурси, властиве зростання кіберзлочинності, зокрема діяльності ботнетів, сервісів ransomware-as-a-service та нелегальних торгових майданчиків у даркнеті. Натомість розвинені демократії й держави, які знаходяться під інформаційним впливом ззовні, мають справу з дуже великими кампаніями дезінформації, маніпулюванням думкою громадськості й втручанням в політичні процеси.

Зрештою, практично для всіх без виключення держав спільний виклик – захист персональних даних та регулювання штучного інтелекту. Масовий витік даних свідчить про недосконаліть наявних систем захисту, в той час, як застосування штучного інтелекту формує нові види загроз, від автоматизованих фішингових атак до генерації шкідливого контенту.

Загалом дослідження показує, що глобальні тенденції кібербезпеки виражаються нерівномірним чином, проте володіють взаємопов'язаним характером: інновації, цифровізація, а також геополітичне протистояння водночас загострюють вразливість і ускладнюють процедури захисту. Це вимагає утворення комплексних стратегій на міжнародному, національному й галузевому рівнях, включно з оновленням нормативно-правової основи, розвитком людських ресурсів, зростанням міжнародної співпраці і введенням сучасних технологій кіберзахисту.

Підсумовуючи усе вищесказане, можемо зробити висновок, що інтеграція штучного інтелекту й людиноцентричних технологій формує нові виклики для кібербезпеки, в тому числі в розрізі захисту від загроз, що мають зв'язок із людським фактором і маніпуляціями штучного інтелекту. Це потребує нових стратегій захисту, які охоплюють як технічні, так і етичні чинники. Захист кіберфізичних систем відіграє дедалі більшу роль, тому що критично значущі системи дедалі більше залежать від взаємодії фізичних і цифрових складових. Це формує додаткові загрози не лише у цифровій, а також і у фізичній сфері. Постійне пристосування до нових загроз – критично значуще для гарантування безпеки на тлі стрімкого технологічного перетворення. Новітні системи кібербезпеки мають стати динамічними й спроможними до самонавчання. Етичні нюанси кібербезпеки в Індустрії 5.0 стають дедалі більше важливими. Застосування штучного інтелекту й персоналізація технологій мають зважати на права особистості, запобігати дискримінації й гарантувати прозорість. Кібербезпека як складова національної безпеки наголошує на потребі напрацювання глобальних та міжнаціональних стандартів для того, щоб боротися із кіберзагрозами, яким

властивий міжнародний характер.

1.2. Сутність та зміст публічного управління у сфері забезпечення кібербезпеки

В нинішніх обставинах швидкої цифровізації й збільшення залежності суспільства від інформаційно-комунікаційних технологій питання забезпечення кібербезпеки відіграє стратегічну роль для національної безпеки країни. Кіберпростір трансформувався в основну інфраструктурну сферу, в якій відбувається велика частина економічних, політичних і соціальних процесів, а його вразливість формує реальні загрози функціонуванню критично важливих систем. Особливо актуальною тема стає на тлі зовнішньої військової агресії проти України, коли кіберпростір виявився одним з головних фронтів бойових дій, а також засобом гібридного впливу. Величезні кібератаки на державні органи, критичну інфраструктуру й приватний сектор показали, що потрібне створення цілісної, адаптивної й проактивної системи публічного управління кібербезпекою, що здатна гарантувати швидке реагування, надійний захист і відновлення цифрових ресурсів.

Відтак зростає роль публічного управління як інструмента, яким формується ефективна державна політика у сфері кіберзахисту, координується діяльність суб’єктів безпеки та забезпечується стійкість в інформаційному середовищі. Погоджуємося з А. Вовк, що «з розвитком цифрових технологій та збільшенням обсягу даних, які обробляються державними органами, кібербезпека стає одним із ключових викликів у публічному управлінні. Урядові системи, бази даних, платформи для надання публічних послуг, а також інформаційні канали стають мішенню для кібератак, які можуть мати катастрофічні наслідки. В умовах постійної загрози з боку зловмисників важливо розробляти та впроваджувати ефективні стратегії захисту, які б забезпечили безперервність роботи державних структур та захист

персональних даних громадян» [19]. Сучасними стратегіями захисту в публічному управлінні є декілька ключових аспектів:

1. «Зміцнення кіберзахисту на рівні державних органів шляхом впровадження передових технологій захисту даних, таких як шифрування, багаторівнева аутентифікація, та використання штучного інтелекту для виявлення аномалій у трафіку.

2. Розвиток кадрового потенціалу шляхом навчання та підвищення кваліфікації працівників державних установ у сфері кібербезпеки, що включає постійне оновлення знань щодо нових видів загроз та методів захисту.

3. Міжнародне співробітництво для обміну інформацією та найкращими практиками у сфері кібербезпеки. Важливо брати участь у глобальних ініціативах та союзах, які спрямовані на протидію кіберзагрозам.

4. Розробка національної стратегії кібербезпеки, яка б враховувала специфічні виклики, пов'язані з безпекою в умовах війни, що передбачає не тільки захист інформаційних систем, але й створення умов для їх швидкого відновлення у разі атаки.

5. Залучення громадян до процесів кібербезпеки, через інформаційні кампанії та освітні програми, що підвищують рівень обізнаності про загрози та способи захисту від них» [185].

Кібербезпека у контексті здійснення публічного управління – один із найбільш вагомих елементів національної безпеки у нинішніх реаліях. Зважаючи на збільшення загроз, які мають зв’язок із кібератаками, потрібно інтегрувати комплексні стратегії захисту, що передбачають як технічні рішення, так і організаційні заходи. Успіх в згаданій галузі залежить від впровадження сучасних технологій, зростання кваліфікованого персоналу й міжнародного співробітництва.

Загалом «кібербезпека» – широко вживане поняття, трактування котрого є дуже поліваріантними, нерідко суб’єктивними й неінформативними. Міжнародний телекомунікаційний союз оперує визначенням, згідно з яким «кібербезпека – це сукупність інструментів, політик, концепцій безпеки,

керівних принципів, підходів до управління ризиками, дій, навчання, найкращих практик, гарантій і технологій, які можуть бути використані для захисту кіберсередовища і активів користувачів» [177].

У Словнику Національної ініціативи з кар'єри та навчання у сфері кібербезпеки Міністерства внутрішньої безпеки США наведено визначення, відповідно до якого кібербезпека – це «діяльність або процес, здатність або можливість, або стан, за допомогою яких інформаційні та комунікаційні системи й інформація, що міститься в них, захищені від пошкодження, несанкціонованого використання, модифікації або експлуатації» [177]. В «Огляді політики Білого дому щодо кіберпростору» наведено визначення кібербезпеки як «стратегії, політики і стандартів, що стосуються безпеки й операцій у кіберпросторі й охоплюють увесь спектр політик і заходів щодо зменшення загроз, зменшення вразливості, стримування, міжнародної взаємодії, реагування на інциденти, забезпечення стійкості та відновлення, зокрема й операцій із комп'ютерними мережами, захисту інформації, правоохоронних, дипломатичних, військових і розвідувальних місій, оскільки вони стосуються безпеки та стабільності глобальної інформаційно-комунікаційної інфраструктури» [196].

О. Бакалінська та О. Бакалинський вважають, що «кібербезпека – захист віртуального середовища, що виникло внаслідок появи Інтернету, а також діяльності людей та організацій на технологічних пристроях та мережах, які до нього підключені» [10]. Л. Веселова розуміє поняття кібербезпека, як «захист критично важливих інфраструктурних послуг, що сприяє основним потребам безпеки, зокрема: безпека інформації стосується захисту конфіденційності; цілісності та доступності інформації загалом, щоб задовольнити потреби відповідного користувача інформації; безпека мережі стосується проектування, впровадження та функціонування мереж для досягнення цілей безпеки інформації в мережах в межах організацій, між організаціями та між організаціями та користувачами; безпека Інтернету стосується захисту послуг, пов'язаних з Інтернетом, та пов'язаних із ними ІКТ-

систем та мереж як розширення безпеки мережі в організаціях та вдома; захист критичної інформаційної інфраструктури займається захистом систем, за допомогою яких об'єктами критичної інфраструктури надаються життєво необхідні послуги: енергетичні, телекомунікаційні системи та водоканали» [17]. На думку Ю. Геращенко кібербезпека – «збір політик та дій, які використовуються для захисту підключених мереж (у тому числі комп'ютери, пристрої, апаратне забезпечення, збережена інформація та інформація, що передається) від несанкціонованого доступу, модифікації, крадіжок, зриву, переривання чи інших загроз» [24].

О. Горун під кібербезпекою розуміє «сукупність інструментів, політик, концепцій безпеки, запевнень в безпеці, настанови, підходи до управління ризиками, дії, навчання, кращі практики, забезпечення та технології, які можна використовувати для захисту кіберсередовища, активів організації та користувача» [28]. Група науковців В. Петрик, М. Присяжнюк та Д. Мельник пропонують власне визначення терміну «кібербезпека». На їх погляд, це «стан захищеності особи, держави та суспільства, за якого забезпечується інформаційний розвиток у технічному, інтелектуальному, соціально-політичному та морально-етичному аспектах, і при цьому зовнішні інформаційні впливи не завдають їм значної шкоди» [110]. Варто наголосити, що згадане трактування містить не тільки пасивний елемент, як-от «ступінь захищеності», а також активний – «інформаційний розвиток», що охоплює технічний, інтелектуальний, соціально-політичний і морально-етичний чинники. О. Ткаченко та К. Ткаченко пропонують наступні визначення поняття «кібербезпека»:

– «кібербезпека – це комплекс належних відповідних способів стосовно зменшення рівня мінімізація ризиків;

– кібербезпека – це охорона кіберфізичних систем від шкідливого та невірного їх застосування, а також від інших руйнівних форсувань;

– кібербезпека – це метод охорони від великої кількості кібернебезпек (до яких відносяться заходи з ушкодження інформаційних ресурсів, вилучення чужих інформаційних даних і т.д.);

– кібербезпека – це охорона інформаційних систем, що відносяться до складу кіберпростору, від нападів, гарантування конфіденційності, цілісності, а також доступності інформаційних даних, які форматуються в цьому просторі, запобігання та боротьба з атаками і кіберзлочинами;

– кібербезпека – охорона кіберфізичних систем від шкідливого невірного застосування і реалізації, а також від інших злочинів» [149].

Варто зауважити, що «теоретичні підходи до публічного управління у сфері кібербезпеки ґрунтуються на стратегічному управлінні, координації дій та розробці державної політики. Дані підходи включають в себе захист національних інтересів, протидія кіберзлочинності, створення необхідної нормативно-правового забезпечення та організацію діяльності національної системи кібербезпеки, зокрема координацію функціонування робочих органів, зокрема Національного координаційного центру кібербезпеки» [147]. Досліджуючи наукові джерела з цієї проблематики, ми вважаємо, слід виділити наступні головні теоретичні підходи до публічного управління у сфері забезпечення кібербезпеки:

1. «Підхід, в основі якого лежить державна політика. Він передбачає розробку та виконання державної політики у сфері кібербезпеки на державному рівні. Це означає ухвалення законодавчих актів, стратегій та програм для захисту національних інтересів та боротьби з кіберзлочинністю.

2. Інституційний підхід – визначає роль державних інституцій, які покликані формувати та реалізувати державну політику у сфері кібербезпеки.

3. Нормативно-правовий підхід, в основі якого лежить створення міцної законодавчої бази для забезпечення кібербезпеки. Це ухвалення законодавчих актів, які регулюють питання кібербезпеки, захисту інформації, електронних комунікацій та боротьби з кіберзлочинністю.

4. Системний підхід, який аналізує кібербезпеку як складний, цілісний комплекс, що складається з взаємопов'язаних елементів, зокрема інформації, інформаційно-комунікаційних систем, суб'єктів забезпечення кібербезпеки, механізмів захисту та поточних загроз. Даний підхід передбачає, що задля забезпечення ефективної кібербезпеки необхідна скоординована взаємодія між усіма частинами системи на національному, регіональному та міжнародному рівнях» [147].

На думку В. Кубанова, кібербезпека системи публічного управління – це «основа національної безпеки, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління» [191]. Розглядаючи кібербезпеку у сфері публічного управління, варто звернути увагу на висловлення Є. Кубанова, який зазначив, що «кібербезпека системи публічного управління – це основа національної безпеки України, яка формує захищеність держави, суспільства, системи публічного управління, населення країни в кібернетичному просторі через створення легітимних механізмів забезпечення кібербезпеки публічного управління» [86].

Незважаючи на повноту визначених підходів, сучасний стан розвитку кібербезпекової сфери обумовлює нові вимоги. Нинішні загрози мають зв'язок із застосуванням штучного інтелекту, машинного навчання, квантових технологій, автономних систем. Таким чином, публічне управління повинне передбачати зростання інновацій, цифрових платформ держави, інтеграцію кіберстійких технологій і передбачення загроз на базі інформації та аналітики. В той же час людський фактор – головне джерело кіберінцидентів. Підходи мають передбачати утворення цифрової культури, зростання компетентностей держслужбовців, освітніх програм й активне спілкування з людьми. Співдія держави з бізнесом, ІТ-компаніями, громадським сектором та міжнародними партнерами – основна. В окреслених підходах недостатнім чином розкривається роль багаторівневого співробітництва й міжсекторальних

механізмів реагування на інциденти. В нинішніх обставинах – насамперед на фоні війни – кіберпростір являється засобом психологічного впливу, інформаційних операцій і маніпуляцій, через це потрібно зважати на когнітивну безпеку, утворення стійкості соціуму до дезінформації, що в наявних підходах не висвітлюється.

Зважаючи на це, пропонуємо більш сучасне та актуальне визначення даного поняття. На наш погляд, під *публічним управлінням у сфері забезпечення кібербезпеки варто розуміти цілеспрямовану, скоординовану та інноваційно орієнтовану діяльність, яка здійснюється органами державної влади, органами місцевого самоврядування та іншими суб'єктами публічної влади, на яку покладено завдання формувати, реалізовувати та оцінювати політики кіберзахисту, забезпечувати кіберстійкість держави, захист цифрового суверенітету, критичної інфраструктури й інформаційного простору, використовуючи нормативно-правові, організаційні, інформаційно-технологічні механізми у взаємодії з приватним сектором, громадянським суспільством та міжнародними інституціями*.

Такий підхід є більш актуальним, оскільки поширення інформаційних операцій, кібератак на інфраструктуру енергетичних систем, банківських мереж, державних реєстрів прямо впливає на рівень обороноздатності, економічної стабільності та ефективність державного управління. До того ж, Україна стала полігоном для поширення нових типів шкідливого програмного забезпечення, проводяться атаки на критичну інфраструктуру; впровадження штучного інтелекту, deepfake-технологій, автономних систем та квантових комп'ютерів змінюють характер кіберзагроз, що вимагає розвитку нових управлінських моделей; з переходом держави на цифрові платформи («Дія», електронні реєстри) виникає необхідність підвищення стійкості кібербезпеки, оскільки виникнення будь-якого збою має масштабні наслідки.

Сфера кібербезпеки складається зі «стандартів, норм, стратегій, принципів формування, засобів реалізації, інструментів управління та запобігання ризикам, що в комплексі формує системний інструментарій

здійснення захисту інформації та даних у кіберсередовищі» [165]. В такій ситуації комплексну сутність кібербезпеки як вектора напрацювання державної політики цифрового розвитку унаочнює нижче презентована схема (рис. 1.1).

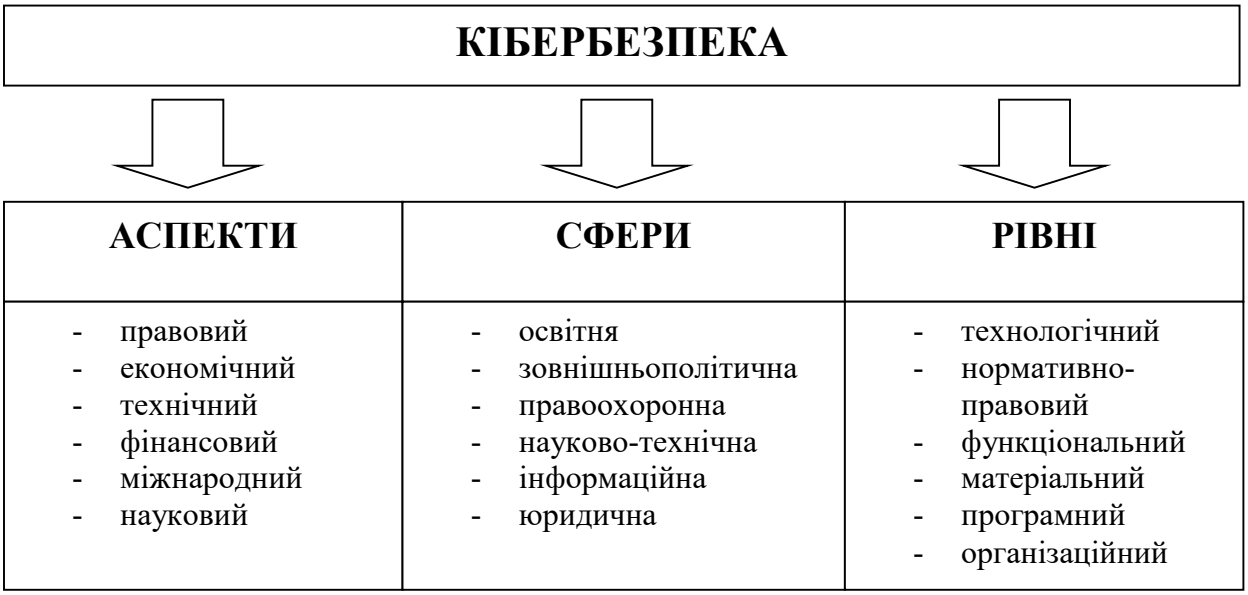

Рис. 1.1. Комплексна сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку

Джерело: розроблено за матеріалами [7]

Як бачимо, кібербезпека в аспекті державної політики цифрового розвитку є системним і багаторівневим феноменом, що охоплює регуляторні, технологічні, організаційні, освітні, міжнародні й фінансові складники. Її комплексність зводиться до впровадження різного роду підходів, засобів і ресурсів, що потрібні для формування безпечної цифрової сфери, яка здатна забезпечити стійке функціонування держави, бізнесу й соціуму. Це не тільки технічний захист інформаційних систем, а також цілісний стратегічний вектор державної політики, орієнтований на зростання цифрової економіки, гарантування цифрового суверенітету, зростання національної безпеки й вироблення стійкості до кіберзагроз.

Правовий аспект визначає формування результативної нормативно-правової основу, що здійснює регуляцію захисту даних, реагування на кіберінциденти, функціонування суб’єктів кібербезпеки, цифрових прав громадян, управління критичною інфраструктурою. Правові механізми

гарантують законність, порядок та стандарти кіберзахисту на національному й міжнародному рівнях. Економічний аспект передбачає утворення передумов для зростання цифрової економіки, інвестицій в кіберзахист, формування конкурентного ринку кіберпослуг, профілактику економічних втрат від кібератак і, крім того, прискорення цифрових інновацій, які покращують ефективність держави й бізнесу. Технічний аспект охоплює технології криптографії, системи встановлення загроз, засоби моніторингу, штучний інтелект для кіберзахисту, хмарні технології, захищені комунікації, технологічне оновлення критичної інфраструктури й зростання її кіберстійкості. Фінансовий аспект має зв'язок з розподілом державних та приватних ресурсів, фінансуванням програм кібербезпеки, створенням відповідних умов для стабільних бюджетних потоків, організацією фондів реагування на кіберінциденти, сприянням інноваційним стартапам і R&D проектам в секторі кіберзахисту. Міжнародний аспект включає участь України у міжнародних угодах, стандартах, співробітництво з НАТО, Європейським Союзом й рештою організацій, спільну протидію кіберзагрозам, обмін інформацією і досвідом, узгодження законодавства зі світовими нормами і інтеграцію в міжнародну систему кібербезпеки. Науковий аспект передбачає зростання досліджень в секторі кіберзахисту, напрацювання інноваційних технологій, сприяння академічним програмам, організацію наукових кластерів, зростання штучного інтелекту й аналітики загроз, що стає основою для новітньої політики цифрового розвитку.

При цьому на рис. 1.1 розкриваються такі сфери реалізації кібербезпеки в державній політиці:

1. Освітня сфера гарантує вироблення цифрової й кібербезпекової компетентності громадян, підготовку спеціалістів із кіберзахисту, зростання STEM-освіти, введення спеціальних курсів у ЗВО, підвищення кваліфікації державних службовців.

2. Зовнішньополітична сфера спрямована на утворення іміджу України як надійного партнера, зростання міжнародного співробітництва, залучення до

міжнародних кіберініціатив, врегулювання кіберінцидентів дипломатичним шляхом і утвердження міжнародної кіберстійкості.

3. Правоохоронна сфера включає роботу кіберполіції, СБУ, решти органів, орієнтовану на розслідування кіберзлочинів, запобігання правопорушенням, створення належних умов для правопорядку в кіберпросторі й захист населення.

4. Науково-технічна сфера створює належні умови для розробки технологій, наукових інновацій, формування кіберзахисних рішень, розвитку наукових парків і лабораторій, які утворюють технологічне підгрунтя безпеки.

5. Інформаційна сфера орієнтована на захист інформаційного сектора, протидію дезінформації, виироблення медіаграмотності й гарантування інформаційного суверенітету країни.

6. Юридична сфера передбачає правове гарантування функціонування всіх суб'єктів кібербезпеки, судовий захист від кіберінцидентів, правове регулювання персональних даних, цифрової ідентифікації, електронних аспектів державного управління.

Також представлено ряд рівнів комплексної системи кібербезпеки:

1. Технологічний рівень включає технічні інструменти захисту, апаратні рішення, криптографію, мережеву безпеку, системи протидії атакам, а також інноваційні технології гарантування кіберстійкості.

2. Нормативно-правовий рівень містить закони, стандарти, стратегії, політики, регулювання роботи суб’єктів кібербезпеки й процедури відповідальності.

3. Функціональний рівень виражає механізми управління, координування суб’єктів, порядки реагування на інциденти, взаємодію органів влади, бізнесу й громадськості.

4. Матеріальний рівень включає фізичні ресурси, зокрема дата-центри, сервери, телекомунікаційне устаткування, інфраструктуру критично важливих об’єктів.

5. Програмний рівень включає програмне забезпечення, цифрові платформи, системи управління ідентифікацією, програмні комплекси виявлення загроз, антивірусні й аналітичні системи.

6. Організаційний рівень встановлює структури управління, моделі взаємодії органів влади, значення суб'єктів системи кібербезпеки, кадрове забезпечення й систему управлінських рішень.

Ефективне управління у цій сфері вимагає чітко визначених завдань, спрямованих на створення стійкої, керованої та здатної до швидкого реагування системи захисту цифрового середовища. Тому важливо визначити ключові завдання, які формують зміст та напрями діяльності суб'єктів публічного управління у сфері кібербезпеки. Завдання системи державного управління кібербезпекою наведено у табл. 1.3. Зауважимо, що «публічне управління відіграє ключову роль у формуванні та реалізації національних стратегій кібербезпеки, забезпечуючи їх ефективне впровадження, моніторинг та адаптацію до динамічних загроз кіберпростору. Важливим аспектом цієї діяльності є координація взаємодії між органами державної влади, приватним сектором та міжнародними партнерами, що сприяє створенню комплексної та стійкої системи кібербезпеки» [96].

Таблиця 1.3

Завдання системи державного управління кібербезпекою

Ключові завдання системи державного управління кібербезпекою України		
1. Оцінка кібербезпеки та кіберзахисту державного органу	2. Оцінка потенційних кіберзагроз на майбутні періоди	3. Формування нормативів забезпечення кібербезпеки державного органу
– аналіз критичних точок; – визначення шляхів здійснення хакерських атак; –ідентифікація найбільш вразливих місць; – аналіз та оцінка хакерських атак минулих періодів	– тестування інформаційної системи; – аналіз розвитку кіберпростору та кіберзлочинності; – оцінка хакерських атак в Україні та світі; – діяльність хакерських груп, та оцінку інших загроз Національній безпеці	– розробка та впровадження Положення про кібербезпеку та кіберзахист державного органу; – впровадження Протоколу протидії хакерським атакам; – розробка та впровадження Положення про оцінку наслідків хакерським атакам
4. Організація системи кіберзахисту	5. Організація безпеки особистих даних	6. Організація кібербпеки робочого місця

– встановленні відповідальних осіб за підтримку кіберзахисту; – організація постійного моніторингу за кіберзагрозами	– забезпечення безпеки особистих даних співробітників	– організація періодичного моніторингу за кіберзагрозами на робочому місці; – визначення порядку дій співробітника
7. Організація кібеззахисту процесів діяльності державного органу	8. Організація системи спеціального зв'язку на випадок несанкціонованого проникнення в інформаційну систему	9. Впровадження протоколу знищення даних на випадок фізичного проникнення
– організація захисту каналів зв'язку між співробітниками	– налагодження системи спеціального зв'язку системи управління	– порядок знищення матеріальних носіїв інформації

Джерело: розроблено за матеріалами [129]

Основні аспекти цієї ролі включають:

1. «Публічне управління має створювати та впроваджувати стратегії кібербезпеки, що визначають пріоритети, цілі та механізми захисту критичної інфраструктури та національних інтересів. Важливим завданням цих стратегій є їх адаптація до динамічного технологічного середовища та еволюції кіберзагроз, що забезпечує гнучкість і стійкість національної системи кібербезпеки.

2. Національна кібербезпека потребує тісної співпраці між різними урядовими структурами, як от Міністерство цифрової трансформації, Міністерство оборони, органи безпеки, правохоронні органи та інші. Ключовим є створення міжвідомчих робочих груп, комітетів або спеціальних агентств для координації дій у сфері кібербезпеки.

3. Державні органи повинні мати можливості для моніторингу кіберпростору, виявлення загроз і атак у реальному часі, а також оцінки рівня готовності та реагування на інциденти. Це включає в себе контроль за критичною інфраструктурою та забезпечення її захисту від потенційних кіберзагроз.

4. Публічне управління повинно забезпечувати належне законодавче забезпечення кібербезпеки, створюючи правові норми для захисту персональних даних, боротьби з кіберзлочинністю, а також для регулювання

діяльності у сфері кібербезпеки. Закони та нормативно-правові акти повинні регулярно оновлюватися з урахуванням нових кіберзагроз та тенденцій.

5. З огляду на глобальний характер кіберзагроз, публічне управління повинно забезпечувати активну взаємодію з міжнародними партнерами, зокрема Європейським Союзом, НАТО, ООН та урядами інших держав. Ця взаємодія охоплює участь у міжнародних ініціативах, спрямованих на обмін інформацією, координацію зусиль у сфері протидії кіберзлочинності та розроблення спільних механізмів реагування на транснаціональні кіберзагрози, що сприяє зміцненню глобальної кіберстійкості.

6. Публічне управління також повинно стимулювати партнерство з приватним сектором, оскільки значна частина критичної інфраструктури знаходиться у приватній власності. Механізми координації між державою та бізнесом повинні включати в себе надання рекомендацій щодо стандартів кібербезпеки, а також взаємодію в разі кіберінцидентів.

7. Державні органи повинні інвестувати в освіту та підвищення кваліфікації кадрів у сфері кібербезпеки. Це включає підготовку фахівців для державних структур, а також для приватного сектору. Залучення освітніх установ до розвитку спеціалізованих програм і курсів має сприяти підвищенню загального рівня кіберграмотності в суспільстві.

8. У разі кіберінцидентів публічне управління повинно мати чіткі плани реагування, в тому числі щодо відновлення функціонування критичної інфраструктури, розслідування кіберзлочинів і мінімізації збитків. Створення спеціалізованих центрів реагування на кіберінциденти (CERT) є важливим елементом національної стратегії» [135].

Більш детально зупинимося якраз на системі заходів гарантування кібербезпеки. Як зазначає О. Труш та Д. Василенко «ефективність функціонування системи забезпечення кібербезпеки насамперед залежить від досконалості нормативно-правового регулювання діяльності відповідної системи державних та громадських органів, а також неурядових організацій» [152]. М. Бондаренко додає, що «законодавчі та нормативні

основи кібербезпеки є одним з основних механізмів формування національної кібербезпеки. Публічне управління повинно створювати чітку правову основу для функціонування системи кібербезпеки, що включає розробку та впровадження законів, стандартів і процедур для захисту інформаційних систем» [14].

При цьому, «до управлінських заходів насамперед слід віднести формування органами публічного управління політики безпеки, що визначають загальний напрям виконання робіт. Організаційно-адміністративне забезпечення кібербезпеки складається з регламентації діяльності та взаємовідносин суб'єктів використання кіберпростору на нормативно-правових засадах, що унеможливлює розголошення, витік і несанкціонований доступ до інформації або створює суттєві труднощі до її доступу за рахунок проведення організаційних заходів. (Наприклад, створення спеціальної служби інформаційної безпеки, визначення посадових інструкцій працівників, організацію режимних заходів, охорону приміщень, контроль за роботою персоналу з інформацією, визначення порядку зберігання, резервування, знищення конфіденційної інформації й т. ін.)» [152].

Важливими є інженерно-технічні (фізичні) заходи, що «являють собою сукупність спеціальних органів, технічних засобів і заходів, що функціонують спільно для виконання певного завдання щодо захисту інформації. Рівень забезпечення кібербезпеки залежить від оточення, в якому працює система забезпечення кібернетичної безпеки. До інженерних засобів відносять екранування приміщень, організація сигналізації, охорона приміщень з персональними комп'ютерами» [152]. При цьому, «програмно-технічні засоби забезпечення кібербезпеки включають в себе апаратні, програмні, криптографічні засоби захисту, які ускладнюють можливість атаки, допомагають виявити факт її виникнення, позбутися від наслідків атаки» [152].

Таким чином, забезпечення кібербезпеки під час ухвалення рішень органами публічного управління є діяльністю, що орієнтована на те, щоб

запобігти, вчасне встановити, припинити або нейтралізувати фактичні та ймовірні загрози під час ухвалення рішень органами публічного управління у процесі застосування кіберпростору через використання законних механізмів забезпечення кібербезпеки.

Що стосується різновидів загроз, то «кіберзагрози для публічного управління можна розділити на кілька основних категорій. Першою є загроза витоку конфіденційної інформації, яка може бути використана для шантажу або підриву довіри до державних інституцій. Другим значним ризиком є атаки на критичну інфраструктуру, що можуть призвести до порушення роботи життєво важливих державних систем, таких як енергетичні мережі, транспорт, зв'язок і фінансові структури. Третя категорія включає атаки на інформаційні системи, які забезпечують роботу органів влади, що може порушити процеси прийняття рішень або управління кризами» [169].

Слід зазначити, що в науковій сфері найпоширеніше класифікувати загрози від сектора утворення. За зауваженням В. Дяченко, з-поміж головних загроз для користувачів під час застосування комп'ютерних мереж виокремлюють низку ризиків, котрі за рівнем припустимості класифікують на: знехтуваний характеризується незначними та допустимими відхиленнями;

– прийнятний в межах характеристик наявної техніки;

– гранично допустимий не повинен перевищуватись ні при яких обставинах;

– надмірний здебільшого, призводить до негативних наслідків» [46].

Серед базових загроз у процесі використання ІТ виокремлюють:

– «комунікаційні ризики, серед яких булінг;

– контентні ризики (матеріали шкідливого характеру);

– споживчі ризики, що пов'язані з порушенням прав споживачів;

– технічні ризики (шкідливі програми тощо)» [46].

Що стосується публічного управління, варто проаналізувати систему основних зовнішніх та внутрішніх загроз кібербезпеки. До зовнішніх загрозам кібербезпеці у ході реалізації публічного управління варто віднести:

– «по-перше, таргетовані атаки. В залежності від цілей, можна виділити дві протилежні тактики атак на комп'ютерні системи. Перший варіант – застосувати для атаки програмне забезпечення (вірус, троянський кінь), маючи на меті компрометацію якомога більшої кількості систем. Другий варіант – проводити атаку прицільно (звідки й назва «таргетовані», тобто націлені), для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією);

– по-друге, кібертероризм (вплив на системи керування). Те, що, власне, і називають кібертерроризмом – можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами. ІКТ надають терористам кілька інструментів: застосування комп'ютерних мереж для керування, координації дій і підготовки терактів; можливість терористам напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету; потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів;

– по-третє, кібервійни. Stuxnet – це є про образ кіберзброї для ведення кібервійни, використовується для здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони);

– по-четверте, хактивізм – зловживання інформацією у соціальних мережах (вплив на суспільство). Як правило, йдеться про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям;

– по-п'яте, атаки на банківські системи (викрадення грошей);

– по-шосте, атаки на електронний уряд. «Електронний уряд» – інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів

державної влади та органів місцевого самоврядування з громадянами та суб’єктами господарювання з метою підвищення ефективності надання державних послуг. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій – підірвати довіру до демократичних перетворень і технічного прогресу» [30].

Внутрішніми загрозами кібербезпеці є: корупційна діяльність, апаратні закладки в мікросхемах та прошивках комп’ютерного й мережного устаткування, слабке налагодження системи управління кіберпростором, неіснування корпоративної політики та ін.

Варто зауважити, що нинішня система публічного управління значним чином спирається на інформаційно-комунікаційні технології, в тому числі в контексті зберігання інформації, надання послуг і комунікації з населенням. Кібератаки чи інші збої у функціонуванні ІКТ-систем здатні завдати суттєвої шкоди системі публічного управління, а також її функціональності, коли зазнають порушень суб’єкт-об’єктні відносини.

Також науковці виділяють різні форми кібератак на систему публічного управління, зокрема:

1. «Фішингові атаки, мета яких – викрасти особисті дані, фінансову інформацію чи отримати доступ до комп'ютерних систем органів публічної влади або заразити комп'ютер користувача шкідливим програмним забезпеченням.

2. DDoS-атаки, їх мета – зробити веб-сайти, онлайн-сервіси недоступними для громадян або вивести з ладу комп'ютерні системи органів публічної влади.

3. Атаки на веб-сайти, мета яких – зламати веб-сайти органів публічної влади, викрасти особисті дані, фінансову інформацію або поширити дезінформацію.

4. Атаки на програмне забезпечення, які спрямовані на – викрадення даних або виведення з ладу комп'ютерних систем органів публічної влади,

використовуючи вразливості в програмному забезпеченні, яке використовується органами публічної влади, щоб отримати доступ до їхніх комп'ютерних систем.

5. Шпигунство, мета таких атак – отримати конкурентну перевагу або отримати конфіденційну інформацію та зашкодити національній безпеці» [41].

Варто зауважити, що кібербезпека в нинішніх обставинах постає не тільки як окрема сфера технічного захисту даних, а як багатовимірне явище, яке пронизує усі галузі життєдіяльності держави та соціуму. Її результативність залежить від спроможності публічної влади впроваджувати різного роду складові управління, ресурси й інститути в єдину цифрову екосистему безпеки. Через це для абсолютного осмислення її суті доречно вивчити кібербезпеку з погляду декількох ключових вимірів, кожний із котрих розкриває своєрідні нюанси утворення, втілення й підтримки державної політики в зазначеній галузі. Зокрема варто виділити:

– «людський вимір є найбільш фундаментальним і, можливо, найбільш слабким елементом кібербезпеки. Хоча кіберпростір побудований на технологіях, людина управляє ними і контролює їх. Оскільки люди є основними акторами, що забезпечують кібербезпека, недостатня поінформованість і недостатні знання роблять людей головною проблемою і найбільш вразливою ланкою в порівнянні з іншими. Крім того, вирішення проблеми нестачі знань не є простим завданням, оскільки вимагає навчання та підготовки протягом певного часу. З цієї причини системи кібербезпеки рекомендують посилення кібербезпеки шляхом підвищення обізнаності, розвитку культури кібербезпеки, а також забезпечення навчання осіб, які займаються питаннями кібербезпеки.

– організаційний вимір зосереджений на інститутах всередині кіберпростору. Це функціональна структура, яка контролює кіберпростір. Зміцнення цього виміру може відбуватись за двома напрямами:

1) стратегічні дії орієнтовані всередині країни, такі як підвищення потенціалу і можливостей відповідної структури;

2) стратегічні дії орієнтовані назовні, які активізують співпрацю для забезпечення безпеки кіберпростору.

– інфраструктурний вимір є, мабуть, найбільш важливим елементом кіберпростору. Це середовище, яке створює кіберпростір. Без інфраструктури кіберпростір – ніщо, тому зміцнення цього виміру необхідно для підтримки кіберсередовища у цілому. Якщо цей вимір слабкий, транзакції в кіберпросторі можуть суттєво знизитись. Тому більшість систем кібербезпеки звертають особливу увагу на інфраструктурні проблеми, у тому числі, на способи забезпечення безпеки критично важливої інформаційної інфраструктури. У цьому сенсі, структура NIST є найбільш придатною для захисту критично важливої інформаційної інфраструктури, але у більшості випадків системи захисту такої інфраструктури відрізняються у різних організаціях, залежно від потреб кожної організації та відповідного кіберпрофілю.

– технологічний вимір розширює можливості кіберпростору. Оскільки кіберпростір включає в себе найбільш передові технології, зміцнення цього виміру в першу чергу означає впровадження новітніх та найбільш ефективних технологій, що забезпечують кібербезпеку і дозволяють проводити подальші дослідження і розробки у цій сфері.

– нормативний вимір структурує кібербезпеку і створює певне імперативне середовище у кіберпросторі. Цей вимір спрямований на формування національної кіберекосистеми шляхом створення нормативно-правової бази та розробки норм і стандартів, а також правозастосування. Хоча деякі стверджують, що кіберпростір не повинний регулюватися і має залишатися вільним від втручання органів влади та політики, правова поведінка все ж необхідна для підтримки стабільності в кіберпросторі» [81].

Отже, сутність публічного управління у сфері забезпечення кібербезпеки зводиться до цілеспрямованої, скоординованої діяльності

публічних органів влади, бізнесу й громадянського суспільства, орієнтованої на те, щоб захищати національні інтереси, громадян і критичну інфраструктуру в кіберпросторі. Згаданий процес передбачає напрацювання політики, нормативно-правове регулювання, заходи організаційного характеру, координацію і контролювання з метою гарантування кіберстійкості держави. В той же час роль публічного управління у сфері забезпечення кібербезпеки складно переоцінити. Воно відіграє критично значущу роль для захисту національних інтересів, стабільного зростання держави й громадської безпеки. Таким чином, публічне управління варто визнати основоположним механізмом, що гарантує не лише захист від кіберзагроз, а також розвиток стабільності, інституційного потенціалу й міжнародної співпраці.

Публічне управління має ключове значення в гарантуванні національної кібербезпеки, допомагаючи результативному здійсненню комплексних заходів, орієнтованих на захист державних і приватних інтересів у цифровій сфері. Важливі компоненти зазначеної процедури – введення механізмів координації між державними органами, моніторинг та контролювання кіберпростору, напрацювання і покращення нормативно-правової основи, міжнародне співробітництво і, крім того, налагодження партнерства із приватним сектором. Узгоджена робота названих механізмів – необхідна передумова для гарантування стабільності й безпеки національної інформаційної інфраструктури, що допомагає зміцнити державну стабільність, сприяє стійкому розвитку й оперативному реагуванню на сучасні кіберзагрози.

1.3. Цифровізація публічного управління як каталізатор розвитку кібербезпеки та ризик-менеджменту у цій сфері

Цифровізація публічного управління стає одним з головних рушіїв модернізації держави, гарантуючи нову якість управлінських механізмів, доступність послуг і прозорість роботи органів влади. Перехід до цифрових

форматів діяльності, введення електронних реєстрів, автоматизованих систем, платформ взаємодії держава–громадянин–бізнес і, крім того, активне застосування штучного інтелекту й аналітичних рішень формують підгрунтя для більш продуктивного функціонування державних структур. В таких обставинах кібербезпека трансформується у невід'ємну складову державної цифрової екосистеми, оскільки збільшення цифрової взаємодії супроводжується зростанням кіберзагроз, ускладненням методів атак і збільшенням цінності інформаційних ресурсів.

Саме цифровізація публічного управління виступає каталізатором розвитку сучасної системи кібербезпеки, тому що створює нові вимоги щодо захисту інформації, заохочує удосконалення державної політики в секторі інформаційної безпеки і гарантує впровадження глобальних стандартів кіберзахисту в національні практики. З однієї сторони, цифрові платформи являються критично значущою інфраструктурою, що вимагає надійних механізмів захисту й оперативного пристосування до нових викликів. З іншої – якраз цифрова трансформація забезпечує змоги для введення новітніх систем моніторингу, реагування й управління інцидентами, організації висококваліфікованих кадрових ресурсів і розвитку культури кібергігієни соціуму.

Впродовж останніх років в Україні дедалі більш активно вводиться цифровізація, поширення й застосування цифрових технологій в організації, а також покращенні роботи органів державного управління й місцевого самоврядування. Стає актуальним питання електронного урядування, налагодження використання інформаційно-комунікаційних технологій в секторі публічного управління на рівні законодавства, тривають наукові дискусії стосовно переваг і викликів цифровізації в наукових дослідженнях, однак частина питань, що мають зв'язок із оцінкою ступеня цифровізації й гарантування передумов для зазначеного процесу вимагають наступного вивчення.

Як зазначає В. Сиротін, «цифровізацією або діджиталізацією розуміється перетворення традиційних аналогових процесів, послуг, або продуктів у цифровий формат. Таке перетворення може застосовуватися у багатьох сферах життя, включаючи бізнес, освіту, медицину, культуру, технології тощо. Основу цифровізації складає інформація, яка обробляється, зберігається і передається за допомогою цифрових технологій, що у підсумку сприяє перетворенню суспільства, економіки і культури в цифрову форму. Активне поширення цифрових технологій та вказані процеси перетворення у суспільстві вплинули й на сферу публічного управління, що виявилось у створенні електронних видів взаємодії між різними учасниками суспільних відносин та спонукають до формування е-урядових інституційних форм у розвинених країнах» [142]. Водночас слід наголосити, що діджиталізація здатна чинити як негативний, так і позитивний вплив на різні сектори життя населення. З-поміж найбільш поширених проблем, що постають у соціумі в результаті активної цифровізації, слід визначити такі:

1. «Збільшення розриву між людьми, які мають доступ до новітніх технологій та навичок цифрової грамотності, і тими, хто не має таких можливостей, що може створювати соціальні і економічні нерівності та обмежити доступ до інформації та можливостей. Цифровізація може змінити вимоги до робочої сили і вимагатиме нових навичок та компетенцій.

2. Заходи цифровізації призводять до збільшення кількості цифрових даних, які потребують захисту від кібератак та зловмисного програмного забезпечення. Вагомого значення в цих питаннях набуває забезпечення ефективного захисту цифрової інфраструктури, щоб запобігти кіберзагрозам. Ці питання кібербезпеки достатньою мірою повинні забезпечуватися державними інститутами, щоб уникнути несанкціонованого витоку інформації, особистих даних, їх продажу та інших дій задля захисту персональних даних громадян.

3. З розвитком нових цифрових технологій можуть з'являтися нові проблеми та виклики, для яких відсутні відповідні регулятивні правила та

процедури. Тому, доцільно створити ефективну регуляторну базу для впровадження та розвитку цифрових технологій» [198, с. 118].

З іншого погляду, «цифровізація має значні переваги, успіх прояву яких залежить від здатності держави ефективно управляти та розвивати національну економіку, зберігаючи при цьому баланс між технологічним прогресом, економічною ефективністю та соціальною справедливістю. Так, у Великобританії для врахування означених проблем та можливостей була розроблена концепція надання публічних послуг, що передбачає розвиток усіх електронних видів сервісу за допомогою мережі Інтернет, мобільного зв'язку, цифрового телебачення або центрів обслуговування та створення системи електронних державних послуг «Електронні громадяни, електронний бізнес, електронний уряд». Створення у Великобританії системи «Електронний уряд» (E-govemment) з метою модернізації публічного управління на основі інформаційних технологій сприяє своєчасності надання інформації про проєкти «електронного уряду» громадянам, підвищенню ефективності та оперативності роботи державного апарату загалом» [198, с. 119]. Один із головних нюансів застосування цифрових технологій зводиться до «удосконалення публічного управління через застосування сучасних інформаційних засобів. На сучасному етапі розвитку інформаційних технологій спостерігається активне використання нових методів і засобів комунікації в роботі органів державної влади та місцевого самоврядування. Світові тенденції також підштовхують уряди розвинутих країн впроваджувати системну цифрову економіку через цифрову трансформацію. Відбувається активна оптимізація національного законодавства, реформа органів державної влади і місцевого самоврядування, а також розробка та впровадження цифрових стратегій, проєктів і програм у сфері державного управління» [8].

При цьому, «цифрова трансформація, як одна з ключових тенденцій у розвитку людської цивілізації, сприяє створенню більш інклюзивного суспільства та поліпшенню механізмів управління. Вона розширює доступ до послуг у сфері охорони здоров'я, освіти та банківського обслуговування,

покращує якість та доступність державних послуг, розширює можливості міжособистої співпраці, а також відкриває можливості для отримання різноманітних товарів за більш доступними цінами» [161].

Цифровізація публічного управління визнається як «процес глибокої перебудови механізмів публічного управління загалом і роботи державних органів у тому числі. Зазначене базується на впровадженні цифрових технологій, які є каталізатором розвитку прогресивних цифрових трансформацій» [136, с. 141]. Зауважимо, що «одним із аспектів цифрової трансформації публічного управляння є електронне урядування. Відмітимо, що електронне урядування в своїй сутнісній основі означає використання цифрових технологій та інтернету для поліпшення ефективності та доступності державних послуг, оптимізації внутрішніх процесів урядування, а також для забезпечення взаємодії між владою та громадянами. Електронне урядування може включати в себе такі елементи, як електронні портали для подачі документів та звернень, електронні системи голосування, цифрові інструменти для моніторингу та оцінки роботи урядових структур, а також використання великих даних для прийняття рішень та багато інших аспектів, що сприяють покращенню якості та доступності державних послуг та публічного управління взагалі» [8]. Під час цифровізації публічного управління вагомий аспект – спрощення та пришвидшення процесів і механізмів ухвалення й виконання державних рішень. Це дає змогу мінімізувати бюрократичні перепони та забезпечити те, що процеси стануть прозорішими й результативнішими. Дякуючи цифровим технологіям, у державних служб з’являється змога оперативніше реагувати на запити населення та покращувати якість наданих послуг. Крім того, вагомий аспект цифрової трансформації – зростання доступності державних послуг для різних категорій громадян, включно з тими, в кого обмежена фізична чи інформаційна мобільність.

Крім того, цифрова трансформація публічного управління дає змогу мінімізувати потенційні прояви корупції шляхом автоматизації процесів і

зведення до мінімуму втручання людей в ухвалення рішень. Електронна ідентифікація громадян і відкриті дані допомагають підвищити прозорість і відкритість роботи державних органів.

У публічному управлінні цифрові технології теж сприяють проведенню аналізу інформації й прогнозуванню, що допомагає більш вдалому ухваленню рішень, основуючись на об'єктивній інформації та дієвому реагуванні на виклики й змоги, які постають в соціумі. Загалом цифрова трансформація публічного управління розширює змоги взаємодії між державними органами, громадянами й підприємствами, робить простішим одержання державних послуг та поліпшує якість життя громадян.

Управління ризиками кібербезпеки є «неодмінною складовою забезпечення безперебійного функціонування інформаційних систем в організаціях будь-якої форми власності. Особливо важливою вона стає в організаціях та державних установах, які для своєї діяльності безпосередньо залежать від мереж і систем інформаційних технологій» [155]. В нинішню цифрову еру управління кіберризиками відіграє вирішальну роль для держави, аби здійснити захист конфіденційної інформації, підтримку відповідності й безперервність діяльності. Зважаючи на збільшення складності й частоти кіберзагроз, органи влади мають використовувати проактивний підхід, щоб результативно виявляти, оцінювати й пом’якшувати ризики.

Управління ризиками – це «процес виявлення вразливостей і загроз інформаційних ресурсів, що використовуються організацією для досягнення цілей і прийняття рішень про те, які контрзаходи, якщо такі є, повинні вживатися задля зниження ризику до прийнятного рівня на основі цінності інформаційного ресурсу для організації» [34, с. 297]. Основні принципи управління ризиками включають:

1. «Ідентифікація. Розуміння потенційних загроз, вразливостей і активів.

2. Оцінка. Аналіз ймовірності та впливу виявлених ризиків.

3. Пом'якшення. Впровадження заходів для мінімізації або усунення ризиків.

4. Моніторинг. Постійний перегляд і оновлення стратегій для адаптації до нових загроз» [154].

Як зазначають В. Федик та Г. Денисенко, «умовно процес управління ризиками можна поділити на три етапи: а) визначення ризиків; Ь) зменшення ризиків; с) оцінка ризиків. Більше того, управління ризиками кібербезпеки передбачає ідентифікацію, оцінку, зниження та контроль ризиків, пов'язаних з кіберзагрозами. Це можливо завдяки впровадженню адекватних заходів технічного, організаційного та правового характеру» [155]. Наприклад, встановлення захисту мереж, застосування новітніх антивірусних програм, своєчасна модернізація складових безпеки програмного забезпечення, постійний аудит систем безпеки, навчання працівників правилам кібербезпеки.

М. Алексєєв робить акцент на тому, що «кібернетичні виклики, з якими сьогодні стикаються державні та недержавні актори, – це складні цільові атаки з боку потужних хакерських об'єднань за якими часто приховуються державні спецслужби; розподілені відмови в наданні послуг (іншими словами DDoS-атаки), які здійснюються за допомогою так званих «ботнетів», що складаються з величезного набору Інтернет-пристроїв, заражених шкідливими програмами та контрольованих злочинними угрупуваннями; застосування кіберзброї, яка здатна виводити з ладу об'єкти критичної інфраструктури» [2, с. 110]. Визначені виклики спричиняють дуже негативні наслідки для економік певних регіонів, цілих держав і, на тлі глобалізації, навіть усього розвинутого світу.

Початковий крок на першій фазі управління ризиками – ідентифікація ризику і його компонентів, як-от потенційних загроз, вразливості і вірогідності в межах конкретно встановленої області. Після цього аналізується вплив зазначеного ризику. Тобто, мета визначення ризику – формування повної характеристики цього ризику й оцінювання її значущості на основі визначених параметрів – опис ризику.

В процесі наступної фази, зважаючи на ймовірний вплив встановлених ризиків, відбувається прийняття рішень стосовно використання чіткої

політики щодо кожного із них. За своєю суттю подібні заходи можуть стати різноаспектними, зокрема юридичними чи адміністративними, організаційними чи процедурними, технічними чи технологічними.

Потім починається етап зменшення ризиків – фаза, на котрій дуже важливо окреслити пріоритети й здійснити раціональний розподіл існуючих ресурсів. Головна мета цього етапу – планування й здійснення заходів, орієнтованих на мінімізацію виявлених ризиків чи контроль над ними, зважаючи на економічну продуктивність.

Після того, як інтегровано заплановані заходи, настає етап оцінки ризиків, що передбачає безперервний моніторинг встановленого ризику й розгляд результативності здійснених заходів. Коли ризик мінімізується до прийнятного рівня, захід визнають вдалим. В іншому разі, чи коли виникає новий ризик, ініціюють новий цикл управління, почавши із першого етапу – визначення ризиків.

Структури кібербезпеки служать структурованими схемами, відповідно до яких організації мають змогу керуватися, аби постійно керувати кіберризиками і послаблювати їх. Вони гарантують систематичний підхід до встановлення вразливостей, оцінювання ризиків та введення інструментів контролю, забезпечуючи те, що всі нюанси управління ризиками кібербезпеки досліджуються в комплексі. Перевагами прийняття структурованої основи в управлінні кібернетичними загрозами є:

1. «Комплексне управління ризиками. Фреймворки пропонують цілісне уявлення про кіберризики, дозволяючи усувати вразливості в усіх системах і процесах.

2. Розширений процес прийняття рішень. Дотримуючись певної структури, можна визначати пріоритетність ризиків на основі їх серйозності, забезпечуючи ефективний розподіл ресурсів.

3. Покращене реагування на інциденти. Рамки часто включають вказівки щодо підготовки, виявлення, реагування на кіберінциденти та відновлення після них, мінімізуючи потенційну шкоду.

4. Масштабованість і адаптивність. Структуровані інфраструктури є універсальними та можуть бути налаштовані відповідно до унікальних потреб користувачів.

5. Довіра зацікавлених сторін. Прийняття визнаних фреймворків демонструє відданість надійній кібербезпеці, посилюючи довіру користувачів, партнерів і регуляторів» [154].

При цьому, технології мають вирішальне значення щодо виявлення, запобігання й реагування на кіберзагрози. Введення правильних технологічних засобів здатне мінімізувати вірогідність вдалої кібератаки й локалізувати шкоду, що обумовлена інцидентом. Ключові технології включають:

1. «Брандмауери діють як бар'єри між внутрішніми мережами та зовнішніми джерелами, фільтруючи трафік, щоб запобігти несанкціонованому доступу та атакам.

2. Шифрування конфіденційних даних гарантує, що навіть якщо дані перехоплено, вони залишаться непрочитаними для неавторизованих осіб. Це критично важливо для захисту конфіденційної інформації під час передачі та зберігання.

3. Системи виявлення вторгнень IDS відстежує мережевий трафік на наявність підозрілих дій і сповіщає команди безпеки про потенційні загрози в режимі реального часу.

4. Захист кінцевої точки, тобто встановлення антивірусних рішень і рішень безпеки кінцевих точок на всіх пристроях гарантує, що будь-які загрози будуть виявлені та пом'якшені на рівні пристрою.

5. Запобігання втраті даних (DLP) контролюють і обмежують переміщення конфіденційних даних, щоб запобігти несанкціонованому доступу або витоку даних» [154].

Стабільна структура управління кібербезпекою дає гарантію того, що управління кіберризиками узгоджується із цілями організації, нормативними вимогами і найбільш вдалими галузевими практиками. Він забезпечує

структуру, що потрібна для результативного управління ризиками й гарантування систематичної відповідності. Ключові елементи включають:

1. «Політика кібербезпеки. Розробка і запровадження політики, яка визначає, як буде керуватися ризиками кібербезпеки, що включає процедури реагування на інциденти, політику прийнятного використання та протоколи захисту даних.

2. Оцінка та управління ризиками. Запровадження формалізованого процесу для регулярної оцінки та управління ризиками кібербезпеки, виявлення нових загроз і визначення відповідних дій для пом’якшення.

3. Ролі та обов'язки. Чітке визначення ролі та обов’язків команд з кібербезпеки, забезпечення підзвітності та ефективності прийняття рішень.

4. Відповідність і дотримання нормативних вимог. Забезпечення умов для дотримання чинних законів і нормативних актів, таких як GDPR, HIPAA та SOX, використовуючи такі рамки, як ISO 27001 або NIST Cybersecurity Framework.

5. Постійний моніторинг і вдосконалення. Встановлення процесів безперервного моніторингу та проведення регулярного аудиту безпеки, з метою оцінювання ефективності засобів контролю кібербезпеки, адаптації до нових загроз» [154].

Узгоджена та структурована система управління кібербезпекою створює фундамент для подальшого формування активних, випереджувальних механізмів реагування на загрози. Логічним продовженням цього є перехід від суто регламентованих процедур до проактивного підходу, який забезпечує не лише контроль за дотриманням політик, а й передбачення можливих ризиків, їх раннє виявлення та запобігання негативним наслідкам у цифровому середовищі.

Науковці зазначають, що «проактивний підхід – це діяльність, що передбачає застосування превентивних і стратегічних заходів з метою формування образу ймовірної події та її наслідків. Загалом, проактивний підхід характеризується стратегічним передбаченням, адаптивністю та

готовністю реагувати на виклики ще до того, як вони переростуть в кризове явище. Поруч із принципом проактивності застосовується системний підхід та активна позиція в управлінській діяльності, спрямована на передбачення та попередження виникнення проблем та негативних наслідків, а також на своєчасну реакцію на зміни у соціальному, економічному, політичному та кібернетичному середовищі. Принцип базується на активному виявленні можливих ризиків, вдосконаленні регулюючих механізмів та використанні інноваційних методів для досягнення позитивних результатів у державному управлінні» [155]. Так, принцип проактивності в першу чергу визначає напрацювання плану реагування на ймовірні надзвичайні ситуації, здійснення постійної і вчасної перевірки конфігурації системи, встановлення ступеня оновлення програмного забезпечення, розгляд результативності системних і програмних обмежень, щоб запобігти несанкціонованому доступу до кіберсистеми, а також її ресурсів, і, крім того, здійснення аудиту системних і мережевих журнальних записів (логів).

У переважному числі ситуацій такий порядок дії дає можливість своєчасно встановити місце утворення ймовірної кібератаки і виявити ресурси, що постраждали. Після цього, щоб відновити нормальний режим діяльності певної кіберсистеми, здійснюються заходи, визначені заздалегідь напрацьованим планом реагування на надзвичайні ситуації.

Як відомо, «до системи управління ризиками входить оцінка ризиків кібербезпеки. Змістовне визначення даному поняттю дає дослідниця Департаменту інформатики Лондонського Королівського коледжу Євгенія Кузьміних, яка підкреслює, що оцінка ризиків інформаційної (кібер) безпеки є важливою частиною практики управління організаціями, що допомагає виявити, кількісно оцінювати та пріоритизовувати ризики з врахуванням критеріїв прийнятності ризиків та цілей, які стосуються конкретної організації чи установи» [186]. Як правило, оцінювання ризиків здійснюється за допомогою методу поєднання анкетування та спільних семінарів при участі фахівців із різних дисциплін чи у рамках окремо сформованої робочої групи

на внутрішньому рівні організації. Оцінка ризику, умовно, може значити «високий», «середній» і «низький» рівні, чи відповідні числові значення на шкалі залежно від необхідної точності, що засновується на суб'єктивних поглядах фахівців стосовно вірогідності і впливу певного ризику.

Під час якісної оцінки ризику кібербезпеки зазвичай застосовується матриця ризиків, у якій на горизонтальній вісі виражається вірогідність утворення певного ризику, а на вертикальній відображається його вплив. В такому разі події із високою вірогідністю і значним впливом посідають верхній правий кут. У той же час ризики, що мають низьку вірогідність і слабкий вплив, розміщені у протилежному куті матриці. Згадана теорія основується на тому, що вища експертна оцінка свідчить про більш значущий параметр. Такий прямолінійний і інтуїтивно доступний прийом вираження гарантує осмислення рівня ризику, насамперед для тих, хто ухвалює рішення, проте не вважається експертами щодо питань безпеки.

В сфері управління ризиками є чотири популярні стратегії:

1. «Стратегія зменшення ризику (подолання негативних наслідків). Цей підхід передбачає встановлення контролю за завданою шкодою та використання компенсаційних заходів, спрямованих на зниження ймовірності виникнення конкретного ризику або пом'якшення його негативних наслідків до прийнятного рівня. У галузі IT такою практикою є регулярне оновлення програмного забезпечення.

2. Трансформація ризику – це практика страхування (перекладання відповідальності за негативні наслідки при реалізації ризиків на іншу сторону). Прикладами використання цієї стратегії є страхування життя або майна. У сфері IT таку роль можуть виконувати Хмарні технології, антивірусні компанії тощо.

3. Прийняття ризику – це практика свідомого допущення роботи системи з відомим ризиком. Багато ризиків з невеликим впливом просто допускаються. Цей підхід також може використовуватися для ризиків, де зменшення негативних наслідків може бути невиправдано дорогим.

4. Уникнення ризику передбачає усунення вразливого елементу системи або, у крайньому випадку, навіть відмову від самої системи» [155].

Аналізуючи доповідь Національного інституту стандартів та технологій США бачимо, що «для задоволення організаційних потреб можна застосовувати три підходи до управління інформаційною безпекою: (а) централізований підхід; (Ь) децентралізований підхід; (с) гібридний підхід. Відповідальність і повноваження щодо прийняття рішень, пов'язаних з інформаційною безпекою та управлінням ризиками, різняться в кожному підході. Структура управління організацією варіюється в залежності від багатьох факторів» [197]. Зокрема:

1. «Централізований підхід. У централізованих структурах управління повноваження, відповідальність і прийняття рішень покладаються виключно на центральні органи. Центральні органи затверджують політику, процедури та правила для забезпечення загально організаційного залучення до розробки та реалізації стратегій управління ризиками та інформаційної безпеки, рішень щодо ризиків та інформаційної безпеки, створення міжорганізаційних та внутрішньо організаційних механізмів комунікації. Централізований підхід до управління вимагає сильного, добре інформованого центрального керівництва, що забезпечуватиме послідовність дій у всій організації. Централізовані структури управління також передбачають меншу автономію для підпорядкованих організацій, які входять до їх структурних підрозділів.

2. Децентралізований підхід. У децентралізованих структурах управління безпекою відповідальність та повноваження щодо прийняття рішень належать та делегуються окремим підпорядкованим органам організації, наприклад, агентства/департаменти в межах виконавчого департаменту федерального уряду або бізнес-підрозділів у межах корпорації. Підлеглі органи встановлюють власну політику, процедури та правила для забезпечення загально організаційної участі в розробці та реалізації стратегій управління ризиками та інформаційної безпеки, рішень щодо ризиків та інформаційної безпеки та створення механізмів для комунікації всередині

такого органу. Децентралізований підхід до управління інформаційною безпекою вміщує підлеглі органи з різними місійними/бізнес/державними потребами та операційними середовищами за рахунок узгодженості всієї організації в цілому. Ефективність такого підходу значно збільшується за рахунок обміну інформацією, пов'язаною з ризиками, між підлеглими органами, щоб жодний підпорядкований орган не зміг передати ризик іншому без інформованої згоди останнього. Важливо також, щоб підпорядковані органи ділилися інформацією, пов'язаною з ризиками, з центральним органом (організацією), оскільки такі ризики можуть мати вплив на організацію в цілому.

3. Гібридний підхід. У гібридних структурах управління безпекою повноваження, відповідальність та прийняття рішень розподіляються між центральним органом(організацією) та окремими підпорядкованими органами. Центральний орган встановлює політику, процедури та правила для забезпечення широкої участі організації в частині стратегій управління ризиками та інформаційної безпеки та рішень, що впливають на всю організацію (наприклад, рішення, пов'язані з спільною інфраструктурою або загальними службами безпеки). Підлеглі органи подібним чином встановлюють відповідні політики, процедури та правила для забезпечення їх участі в частині стратегій управління ризиками та інформаційної безпеки та рішень, які є специфічними для їхніх потреб та середовища діяльності. Гібридний підхід до управління вимагає сильного, добре інформованого керівництва не лише в центральному органі, але й в підпорядкованих йому органах, з метою забезпечення послідовності щодо управління ризиками та безпекою у всій організації» [197].

Кожен із цих підходів визначає, хто саме несе відповідальність за політики, рішення та моніторинг: чи це централізований центр прийняття рішень, чи розподілена мережа відповідальних підрозділів, чи поєднання обох моделей. Саме через призму цих підходів стає зрозумілим, як різні структури управління можуть впливати на ефективність кібербезпеки, гнучкість

реагування на загрози, а також рівень уніфікації та контролю. Відтак, підсумуємо основні особливості управління ризиками кібербезпеки в умовах цифровізації публічного управління (табл. 1.4).

Таблиця 1.4

Особливості управління ризиками кібербезпеки в умовах цифровізації публічного управління

Аспект	**Зміст**	**Прояв у практиці публічного управління**	**Ключові наслідки / ризики**
1. Зростання цифрової залежності	Поширення цифрових сервісів і баз даних у сфері публічного управління	Впровадження електронних реєстрів, документообігу, автоматизація процесів, використання хмарних сервісів	Підвищується вразливість держави до кібератак, з'являються ризики скорочення темпів розвитку цифрових послуг
2. Ускладнення кіберзагроз	Комплексність атак шляхом застосування AI-технологій та соціальної інженерії	Поширення фішингу проти державних службовців, DDoS-атак на сервіси, атак на критичну інфраструктуру	Зростання високих збитків, поширення компрометації даних, ризиків порушення національної безпеки
3. Нерівномірність цифрової зрілості органів влади	Урізноманітнення технічного оснащення та культури безпеки	Володіння деякими органами розвиненою інфраструктурою кіберзахисту, включаючи SOC-центри та комплексні політики безпеки, тоді як для інших характерна наявність лише мінімальних, базових заходів захисту.	Створення слабкими ланками влади вразливостей для всієї державної системи
4. Інтеграція нових технологій	Використання хмарних технологій, штучного інтелекту, Big Data, IoT, що вимагає розробки нових підходів до безпеки	Підключення сенсорів, автоматизованих систем, прогнозної аналітики	Поширення ризиків некоректної роботи, втручань у системи, кібервитоків даних
5. Потреба в міжвідомчій координації	Виникнення потреби в узгодженні	Обмін даними між міністерствами, впровадження	Підвищення випадків фрагментарності,

	стандартів та процедур	інтегрованих реєстрів, спільної політики	повторення інцидентів, низької ефективності реагування
6. Людський фактор як ключовий елемент ризику	Недостатність кіберграмотності працівників, нехтування безпековими правилами	Встановлення слабких паролів, наявність відкритих листів фішингу, ненавмисне поширення інформації	Поширення інцидентів, спричинених людськими помилками
7. Необхідність динамічного управління ризиками	Швидка зміна класифікації ризиків, що робить класичні підходи недостатніми	Наявність потреби в постійному моніторингу, актуалізації політики	Підвищення ризику того, що використання застарілих моделей безпеки більше не гарантує захисту
8. Брак кадрів і компетенцій	Наявність кадрового дефіциту у державному секторі у сфері кібербезпеки	Відсутність спеціалістів та аналітиків, що володіють ефективними навичками кібербезпеки	Підвищення ризику нездатності до оперативного реагування на інциденти та розбудови систему безпеки
9. Підвищені вимоги до захисту персональних даних	Розширення цифрових реєстрів, що призводить до збільшення обсягу чутливої інформації	Впровадження Е-реєстрів, цифрових послуг, систем автоматизованого прийняття рішень	Зростання ймовірності витоку даних, правових наслідків, втрати довіри громадян
10. Необхідність комплексного, багаторівневого підходу	Виникнення необхідності керування ризиками на стратегічному, технічному, організаційному рівнях	Наявність необхідності впровадження політики, стандартів, аудиту, ризик-менеджменту, резервування	Забезпечення стійкості державної цифрової інфраструктури

Джерело: власна розробка автора

Як бачимо, цифрова трансформація державного сектору обумовлює те, що безпековий компонент стає не просто значущим, а визначальним для стабільності і стійкості державних інституцій. Розгляд кожної групи характерних ознак дає можливість зрозуміти системність ризиків і необхідність щодо цілісної політики кіберзахисту.

Насамперед, цифровізація істотно збільшує залежність органів влади від інформаційно-комунікаційних технологій. Перехід на електронні реєстри,

хмарні платформи й автоматизовані системи обумовлює нові точки вразливості, оскільки будь-який збій чи атака здатні виводити з ладу державні сервіси. Це має прямий зв’язок із тим, що кіберзагрози ускладнюються, оскільки наразі основуються на застосуванні штучного інтелекту, автоматизованих бот-мереж і методів соціальної інженерії. Подібний хід дій ставить перед державою вимогу щодо оперативної модернізації інструментарію реагування і введення адаптивних моделей безпеки.

Крім того, цифрова трансформація, поглиблює проблему нерівномірності цифрової зрілості органів влади, оскільки одні установи показують високі стандарти захисту, інші продовжують залишатися вразливими з огляду на обмежені потенціал або людські ресурси. Якраз згадані «слабкі ланки» робляться можливими точками входу для кібератак на загальнодержавні системи. Додаткова складність – впровадження нових технологій, як-от IoT, великі дані або штучний інтелект, котрі, з однієї сторони, покращують результативність управління, проте з іншої формують додаткові поверхні для атак.

Управління ризиками кібербезпеки вимагає тісної міжвідомчої взаємодії. Без єдиних стандартів, уніфікованих політик і координації заходів безпеки навіть найбільш інноваційні технології не можуть забезпечити відповідний захист. Людський фактор продовжує залишатися однією з головних інцидентів: недостатній рівень кіберграмотності працівників, порушення політик безпеки або необережне поводження з даними формують значні загрози навіть у високотехнологічній сфері.

Крім того, сучасні ризики мають динамічний характер, що робить класичні статичні моделі безпеки неефективними. Державні органи повинні здійснити перехід до гнучких систем моніторингу й системних аудитів. Проблема ускладнюється з огляду на постійний кадровий дефіцит у сфері кібербезпеки, через що обмежуються змоги держави швидко реагувати на інциденти й здійснювати розвиток інституційної спроможності.

Зростання кількості електронних реєстрів підсилює вимоги до захисту персональних даних. Витоки будь-якого характеру здатні не тільки шкодити населенню, а також підривати довіру до цифровізації в цілому. Врешті-решт дієве управління ризиками кібербезпеки ймовірне тільки в разі комплексного багаторівневого підходу, котрий включає стратегічні, організаційні, технічні й кадрові чинники, що дає можливість утворювати стійку систему кіберзахисту, яка є відповідною новітнім викликам і гарантує постійність функціонування цифрової держави.

Таким чином, цифровізація публічного управління являє собою застосування цифрових технологій і потенціалу онлайн-комунікацій під час ухвалення і виконання публічних управлінських рішень, надання адміністративних послуг і, крім того, створення дієвих інструментів введення державної політики в усіх секторах життя суспільства. Цифрові технології орієнтовані на якнайбільше зменшення часу передавання інформаційних повідомлень від державних органів до кінцевих користувачів шляхом ефективного застосування цифрового простору. По-перше, це робить простішим процес одержання важливих публічних послуг і дозвільної документації для людей, по-друге, мінімізує фінансові витрати на обслуговування системи надання публічних послуг в офлайн-режимі, та, по-третє, зменшує вияви корупції, тому що немає прямого контакту між надавачем публічних послуг і громадянином.

Стосовно публічного управління, то процес цифровізації здатний містити різні зміни в усталених практиках, технологіях і механізмах, як-от переведення державних послуг в електронний формат, застосування нових засобів державної комунікації, надання документів через мережу «Інтернет», зростання стійкого співробітництва між органами влади та громадськістю за допомогою електронних сервісів й інших ініціатив.

Синергетичні можливості соціальних, мобільних, хмарних технологій, технологій вивчення інформації й Інтернету речей спільно мають ресурс спричиняти трансформаційні зміни в державному управлінні і загалом

встановити його результативність, реактивність і цінність. Новітні цифрові технології здійснюють вплив на соціальні, культурні, комерційні й адміністративні структури і крім того, на спосіб, за допомогою котрого люди взаємодіють, комунікують і співпрацюють, і, до того ж, як вони розуміють і застосовують інформацію. Це забезпечує нові змоги для доступу до інформації, обміну знаннями і взаємодії між громадянами й організаціями.

Спрощений доступ до публічних послуг і документів через мережу «Інтернет» сприяє зростанню якості життя людей, допомагає транспарентності й дієвості публічного управління. Зростання цифрових інструментів та процесів співробітництва між органами влади та громадськістю допомагає вдосконалити взаємодію і збільшити ступінь задоволеності населення державними послугами. Цифрові технології й інтернет дають можливість формувати нові форми доступу до інформації, а також взаємодії, збільшуючи потенціал співробітництва та конкуренції у соціумі. Таким чином, новітні цифрові технології допомагають не тільки модернізації публічного управління, а також трансформують власне спосіб функціонування суспільства і взаємодії між його учасниками.

Що стосується ефективного управління ризиками кібербезпеки, це більше не вважається необов’язковим, це критична потреба в нинішній цифровій ері. Визнаючи структуровані рамки, здійснюючи грунтовну оцінку ризиків та інтегруючи найбільш вдалі практики, організації мають можливість пом’якшити загрози, гарантувати відповідність та захистити власні важливі активи. Проте, щоб цього досягти, необхідні правильні інструменти й стратегії, які розроблено, щоб розв’язати нові проблеми кібербезпеки.

Висновки до розділу 1

1. Виявлено, що впровадження штучного інтелекту й людиноцентричних технологій обумовлює нові виклики для кібербезпеки, в тому числі в розрізі захисту від загроз, що мають зв’язок із людським фактором

і маніпуляціями штучного інтелекту. Це ставить вимогу щодо нових стратегій захисту, які охоплюють як технічні, так і етичні аспекти. Захист кіберфізичних систем відіграє дедалі більшу роль, тому що критично важливі системи дедалі більше залежать від взаємодії фізичних і цифрових складових. Це формує додаткові загрози не лише у цифровій, а також у фізичній сфері. Постійне пристосування до нових загроз вважається критично значущим для гарантування безпеки на тлі стрімкого технологічного перетворення. Новітні системи кібербезпеки мають стати бути динамічними і спроможними до самонавчання. Етичні аспекти кібербезпеки в Індустрії 5.0 стають дедалі більш вагомими. Застосування ШІ й персоналізація технологій мають зважати на права людини, запобігати дискримінації й гарантувати прозорість. Кібербезпека як елемент національної безпеки акцентує на потребі напрацювання глобальних та міжнаціональних стандартів для того, щоб боротися з кіберзагрозами, яким властивий глобальний характер.

2. Вивчено сутність та зміст публічного управління у сфері забезпечення кібербезпеки. Під публічним управлінням у сфері забезпечення кібербезпеки запропоновано розуміти цілеспрямовану, скоординовану та інноваційно орієнтовану діяльність, яка здійснюється органами державної влади, органами місцевого самоврядування та іншими суб’єктами публічної влади, на яку покладено завдання формувати, реалізовувати та оцінювати політики кіберзахисту, забезпечувати кіберстійкість держави, захист цифрового суверенітету, критичної інфраструктури й інформаційного простору, використовуючи нормативно-правові, організаційні, інформаційно-технологічні механізми у взаємодії з приватним сектором, громадянським суспільством та міжнародними інституціями. Такий підхід є більш актуальним, оскільки поширення інформаційних операцій, кібератак на інфраструктуру енергетичних систем, банківських мереж, державних реєстрів прямо впливає на рівень обороноздатності, економічної стабільності та ефективність державного управління. До того ж, Україна стала полігоном для поширення нових типів шкідливого програмного забезпечення, проводяться

атаки на критичну інфраструктуру; впровадження штучного інтелекту, deepfake-технологій, автономних систем та квантових комп’ютерів змінюють характер кіберзагроз, що вимагає розвитку нових управлінських моделей; з переходом держави на цифрові платформи («Дія», електронні реєстри) виникає необхідність підвищення стійкості кібербезпеки, оскільки виникнення будь-якого збою має масштабні наслідки.

3. З'ясовано, що ефективне управління ризиками кібербезпеки в умовах цифровізації публічного управління вимагає комплексного й збалансованого підходу, що зважає як на технологічні, так і на організаційні, кадрові й правові чинники. Цифрова трансформація відкриває великий потенціал для покращення результативності державних процесів, проте водночас утворює нові напрями вразливостей, що мають зв’язок як зі збільшенням кількості цифрової інформації, так і з ускладненням новітніх кіберзагроз. Нерівномірність ступеня кіберзахисту в різних органах влади, брак кваліфікованого персоналу, стрімка зміна ризиків й динамічне введення сучасних технологій обумовлюють те, що система державної кібербезпеки стає структурно чутливою і вимагають інтенсивної міжвідомчої координації. В той же час держава повинна особливу увагу сконцентровувати на зростанні культури кібергігієни й відповідальності працівників, оскільки людський фактор продовжує залишатися однією із найбільш слабких складових безпекового контуру. Гарантування надійного захисту персональних даних та критичних цифрових платформ – головна умова підтримки довіри людей до цифрових сервісів і до процесу цифровізації у цілому. В зазначеному розрізі стратегічною потребою стає інтеграція новітніх методик ризик-менеджменту, динамічних моделей моніторингу й уніфікованих державних стандартів кіберзахисту.

РОЗДІЛ 2
СУЧАСНИЙ СТАН РЕАЛІЗАЦІЇ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

2.1. Механізми публічного управління у сфері забезпечення кібербезпеки України

В нинішніх обставинах, коли відбувається цифровізація суспільних процесів і стрімко розвиваються інформаційно-комунікаційні технології, кіберпростір став одним з головних аспектів національної безпеки держави. Для України питання забезпечення кібербезпеки стає по-особливому актуальним на тлі гібридної війни, збільшення кількості кібератак на об’єкти критичної інфраструктури, державні інформаційні ресурси, а також системи електронного урядування. Кіберзагрози все частіше застосовуються як засіб політичного, економічного й інформаційного тиску, що ставить вимогу стосовно системної й скоординованої реакції зі сторони органів публічної влади.

Результативне забезпечення кібербезпеки не може відбуватися без утворення й втілення ефективних механізмів публічного управління і, крім того, взаємодії держави із приватним сектором та громадянським суспільством. Якраз публічне управління зобов’язане гарантувати цілісність державної політики в секторі кібербезпеки, узгодженість дій суб’єктів кіберзахисту й пристосування управлінських рішень до інтенсивних викликів цифрового простору.

В зазначеному аспекті розгляд механізмів публічного управління у сфері забезпечення кібербезпеки України вважається вагомим у науковому й практичному вимірах. Він допомагає поглибити теоретико-методологічні принципи державного управління в секторі національної безпеки і, крім того, напрацювати пропозиції стосовно покращення управлінських інструментів

протидії кіберзагрозам на тлі воєнного стану й відновлення держави після війни.

Насамперед розглянемо *нормативно-правовий механізм* у сфері забезпечення кібербезпеки України. Законодавчою основою у цій сфері є наступний перелік законів України, постанов Кабінету Міністрів України та інших нормативних документів.

1. Закон України «Про основні засади забезпечення кібербезпеки України», який «визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки» [129]. Даний Закон не поширюється на:

1) «відносини та послуги, пов’язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах;

2) соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов’язані з функціонуванням таких мереж і ресурсів;

3) комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)» [129].

2. Закон України «Про оборону України» [128] закріплює обов'язковість реалізації заходів із кібероборони, щоб захистити суверенітет держави й гарантувати її обороноздатність, запобігти збройному конфлікту й дати відсіч збройній агресії, зокрема – здійснення спеціальних операцій (розвідувальних,

інформаційно-психологічних та ін.) в кіберпросторі під час підготовки до захисту й захисту України у випадку збройної агресії. Зацікавлює те, що обов'язковість реалізації подібних заходів передбачається у мирний період під час підготовки держави до оборони, однак прямі кроки, котрі слід робити в аспекті кібероборони в ході протистояння збройній агресії, в згаданому законі не відображаються.

3. Закон України «Про національну безпеку України», який «визначає основи та принципи національної безпеки і оборони, цілі та основні засади державної політики, що гарантуватимуть суспільству і кожному громадянину захист від загроз та сприятимуть утвердженню української національної та громадянської ідентичності. Цим Законом визначаються та розмежовуються повноваження державних органів у сферах національної безпеки і оборони, створюється основа для інтеграції політики та процедур органів державної влади, інших державних органів, функції яких стосуються національної безпеки і оборони, сил безпеки і сил оборони, визначається система командування, контролю та координації операцій сил безпеки і сил оборони, запроваджується всеосяжний підхід до планування у сферах національної безпеки і оборони, забезпечуючи у такий спосіб демократичний цивільний контроль над органами та формуваннями сектору безпеки і оборони» [126].

4. Закон України «Про ратифікацію Конвенції про кіберзлочинність» [130], який вважається не тільки інструментом міжнародно-правової інтеграції, а також значущою складовою механізмів публічного управління у сфері забезпечення кібербезпеки України. Він допомагає системності державної політики, покращенню результативності управлінських рішень, посиленню інституційної спроможності органів влади й виробленню комплексного підходу щодо протидії кіберзагрозам на тлі нинішніх безпекових викликів.

5. Закон України «Про інформацію», який «регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації» [124].

6. Закон України «Про Державну службу спеціального зв’язку та захисту інформації України» «відповідно до Конституції України визначає правові основи організації та діяльності Державної служби спеціального зв’язку та захисту інформації України» [114]. У Законі зазначається, що на Державну службу спеціального зв’язку та захисту інформації України відповідно до визначених завдань покладаються такі обов’язки у контексті забезпечення кібербезпеки:

– «визначення для виконання завдання щодо функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози:

– встановлення для виконання завдання щодо функціонування національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози:

– запровадження організаційно-технічних заходів щодо створення національної системи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози;

– забезпечення функціонування платформи обміну інформацією про кіберінциденти, кібератаки, кіберзагрози та встановлення порядку приєднання до такої платформи» [114].

7. Закон України «Про електронні комунікації», який «визначає правові та організаційні основи державної політики у сферах електронних комунікацій та радіочастотного спектра, а також права, обов’язки та відповідальність фізичних і юридичних осіб, які беруть участь у відповідній діяльності або користуються електронними комунікаційними послугами» [115]. У Законі одним із завдань державного управління і регулювання у сферах електронних комунікацій та радіочастотного спектра визначено «підтримку безпеки електронних комунікаційних мереж і послуг» [115].

8. Постанова Кабінету Міністрів України від 16.11.2002 № 1772, якою затверджено «Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах», який «визначає механізм взаємодії органів виконавчої влади з

питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних системах» [119].

9. Постанова Кабінету Міністрів України «Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем» від 29.03.2006 № 373. Відповідно до постанови мінімальні вимоги «визначають сукупність організаційних та технічних вимог до заходів захисту інформації та кіберзахисту, що підлягають впровадженню органами державної влади, іншими державними органами, органами місцевого самоврядування, державними підприємствами, установами та організаціями, які є власниками або розпорядниками інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем (далі – система), в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом» [117].

10. Постанова Кабінету Міністрів України від 09.10.2020 № 943, якою затверджено «Деякі питання об'єктів критичної інформаційної інфраструктури», що «визначає механізм формування національного та секторальних переліків об’єктів критичної інформаційної інфраструктури. Дія цього Порядку не поширюється на банки, інші юридичні особи, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг» [39].

11. Постанова Кабінету Міністрів України від 25.06.2025 № 761, якою затверджено «Правила надання та отримання електронних комунікаційних послуг», які «регулюють відносини між постачальниками електронних комунікаційних послуг (далі – постачальники послуг) та кінцевими користувачами електронних комунікаційних послуг (далі – кінцеві користувачі) і визначають порядок надання та отримання електронних комунікаційних послуг» [123].

12. Постанова Кабінету Міністрів України від 19.06.2019 № 518 «Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури». Ці Загальні вимоги «визначають організаційно-методологічні умови кіберзахисту об’єктів критичної інфраструктури, що є обов’язковими до виконання операторами критичної інфраструктури та власниками або розпорядниками об’єктів критичної інформаційної інфраструктури. Дія цих Загальних вимог не поширюється на Національний банк, банки, інші установи та осіб, що провадять діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, а також на операторів платіжних систем, їх учасників та технологічних операторів платіжних послуг» [116].

13. Постанова Кабінету Міністрів України від 23.12.2020 № 1295 «Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки». Цей Порядок «визначає засади функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, які здійснюються щодо об’єктів кіберзахисту, визначених частиною другою статті 4 Закону України «Про основні засади забезпечення кібербезпеки України». Особливості функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки у банківській системі України визначаються Національним банком. Дія цього Порядку не поширюється на об’єкти критичної інформаційної інфраструктури Міноборони та Збройних Сил в умовах надзвичайного і воєнного стану» [38].

14. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» від 26 серпня 2021 року № 447/2021», де зазначається, що «забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України. Реалізація зазначеного пріоритету буде здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі» [131].

Відповідно до Стратегії, для подальшої розбудови національної системи кібербезпеки на засадах стримування, кіберстійкості, взаємодії необхідним є:

– «посилення спроможності національної системи кібербезпеки для унеможливлення збройної агресії проти України у кіберпросторі або з його використанням, нейтралізації розвідувально-підривної діяльності, мінімізації загроз кіберзлочинності та кібертероризму (стримування);

– набуття здатності швидко адаптуватися до внутрішніх і зовнішніх загроз у кіберпросторі, підтримувати та відновлювати стале функціонування національної інформаційної інфраструктури, насамперед об'єктів критичної інформаційної інфраструктури (кіберстійкість);

– забезпечення розвитку комунікації, координації та партнерства між суб'єктами забезпечення кібербезпеки на національному рівні, розвиток стратегічних відносин у сфері кібербезпеки із ключовими іноземними партнерами, передусім з Європейським Союзом, Сполученими Штатами Америки та іншими державами – членами НАТО, співробітництво у цій сфері з іншими державами та міжнародними організаціями на основі національних інтересів України (взаємодія)» [131].

Окрім ключових суб'єктів національної системи кібербезпеки, Україна буде залучати до розв’язання завдань у згаданому секторі значно ширше коло учасників, зокрема суб'єкти господарювання, громадські об'єднання й певних громадян України.

15. Наказ Адміністрації Держспецзв’язку від 10.06.2008 № 94, яким затверджено «Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»; наказ зареєстровано в Міністерстві юстиції України 07.07.2008 за № 603/15294. Цей Порядок «визначає механізм координації діяльності органів державної влади, органів місцевого

самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності (далі – суб'єкти координації) з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах (далі – ІКС), виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІКС. Метою цього Порядку є організація координації діяльності з питань запобігання вчиненню порушень безпеки інформації в ІКС, виявлення та усунення наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в ІКС, а також впровадження єдиної процедури надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в ІКС» [120].

16. Наказ Адміністрації Держспецзв’язку від 02.12.2014 № 660, яким затверджено «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах»; наказ зареєстровано в Міністерстві юстиції України 28.01.2015 за № 90/26535. Цей Порядок «визначає правові та організаційні засади проведення оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності» [121].

17. Наказ Адміністрації Держспецзв’язку від 15.01.2016 № 20, яким затверджено «Порядок сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті»; наказ зареєстровано в Міністерстві юстиції України 05.02.2016 за № 196/28326. Цей порядок «визначає організаційні засади проведення сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет» [122].

Незважаючи на значний перелік нормативно-правових актів, варто виділити основні проблеми нормативно-правового забезпечення у сфері публічного управління кібербезпекою України:

1. Фрагментарність та несистемність нормативно-правової бази. Нормативно-правові акти в секторі кібербезпеки приймалися нерівномірним чином і нерідко як реагування на певні загрози, що спричинило відсутність цілісної й ієрархічно узгодженої системи правового регулювання.

2. Нечіткість розмежування повноважень суб'єктів публічного управління. В законодавстві продовжує зберігатися дублювання чи розмитість компетенцій між органами державної влади, в тому числі в питаннях кіберзахисту, реакції на ситуації й координування дій в кризових випадках.

3. Недостатній рівень гармонізації з міжнародними та європейськими стандартами. Незважаючи на ратифікацію міжнародних конвенцій, деякі норми національного законодавства не повністю узгоджено з вимогами Європейського Союзу, стандартами НАТО й новітніми підходами до управління кіберризиками.

4. Відставання правового регулювання від темпів технологічного розвитку. Законодавство не поспіває за динамічним розвитком цифрових технологій, штучного інтелекту, хмарних сервісів та нових видів кіберзагроз, через що зменшується його результативність під час практики.

5. Обмежена регламентація публічно-приватного партнерства у сфері кібербезпеки. Нормативно-правові акти недостатнім чином здійснюють врегулювання механізмів взаємодії органів влади із приватним сектором, що має велику частину критичної інформаційної інфраструктури.

6. Недостатня деталізація процедур реагування на кіберінциденти та кіберкризи. Немає єдиних стандартизованих правових алгоритмів дій органів публічної влади в обставинах глобальних кібератак, через що ускладнюється швидкість і узгодженість управлінських рішень.

7. Неврегульованість питань кібербезпеки на регіональному та місцевому рівнях. Нормативно-правове забезпечення публічного управління у

сфері кібербезпеки зосереджується в основному на центральному рівні, що лімітує здатність органів місцевого самоврядування.

8. Обмеженість правових інструментів забезпечення кіберстійкості в умовах воєнного стану. Діюче законодавство не повністю бере до уваги своєрідність гібридних загроз та потребу щодо специфічних правових режимів управління кібербезпекою у ході збройної агресії.

Наявні проблеми нормативно-правового забезпечення у сфері публічного управління кібербезпекою України вказують на потребу його наступного системного вдосконалення, зважаючи на новітні безпекові виклики, динаміку цифрової трансформації й умови воєнного стану. Усунення фрагментарності законодавства, чіткий розподіл повноважень суб'єктів публічної влади, узгодження національних норм з міжнародними стандартами і введення дієвих механізмів координації та відповідальності повинні стати головними завданнями державної політики в зазначеній галузі.

Розглядаючи *організаційний механізм* публічного управління у сфері забезпечення кібербезпеки, варто зауважити, що суб'єкти забезпечення кібербезпеки, діючи у рамках повноважень, які їм надані, реалізують комплексну діяльність, націлену на те, щоб не допустити використання кіберпростору на користь воєнної агресії, розвідувально-підривних, терористичних й інших протиправних дій, та, крім того, на вчасне встановлення кіберінцидентів і кібератак, реагування на них і зведення до мінімуму їхніх наслідків негативного характеру. Значущий елемент зазначеної діяльності – налагодження регулярного інформаційного обміну стосовно існуючих та ймовірних кіберзагроз, розробки і введення превентивних, організаційних, освітніх та захисних заходів у секторі кібербезпеки, кібероборони та кіберзахисту. До того ж такі суб'єкти гарантують виконання аудиту інформаційної безпеки на об'єктах, які знаходяться в секторі їхнього управління, і, крім того, здійснюють решту управлінських і практичних заходів, орієнтованих на стабільне зростання та безпечне функціонування кіберпростору України.

Діяльність в секторі кібербезпеки як елемента національної безпеки України координується Президентом України, яким очолюється Рада національної безпеки і оборони України.

Відповідно до законодавства, до суб'єктів, якими безпосередньо здійснюється комплекс заходів із забезпечення кібербезпеки є:

1) «міністерства та інші центральні органи виконавчої влади;

2) місцеві державні адміністрації;

3) органи місцевого самоврядування;

4) правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності;

5) Збройні Сили України, інші військові формування, утворені відповідно до закону;

6) Національний банк України;

7) оператори критичної інфраструктури та власники або розпорядники об'єктів критичної інформаційної інфраструктури;

8) суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом» [129].

Кабінет Міністрів України [61] є головним суб'єктом публічного управління у сфері кібербезпеки, гарантуючи розробку й практичне втілення державної політики в зазначеному секторі, націленої на захист прав та свобод людини й громадянина, національних інтересів держави у кіберпросторі та протидію кіберзлочинності. В рамках своїх повноважень Уряд гарантує діяльність національної системи кібербезпеки, мобілізуючи потрібний організаційний, кадровий, фінансовий і технічний потенціал, і, крім того, ухвалює національний план реагування на кіберінциденти і кібератаки. Вагомий елемент його функціонування – визначення загальних вимог щодо кіберзахисту об'єктів критичної інфраструктури і встановлення механізмів

оцінки стану кіберзахисту інформаційних та телекомунікаційних систем, в котрих здійснюється обробка державних інформаційних ресурсів, службових даних чи інформація, яка вважається державною таємницею. Також Кабінет Міністрів України встановлює алгоритм взаємодії між суб'єктами національної системи реагування на кіберзагрози, органами гарантування кібербезпеки, правоохоронними, розвідувальними й контррозвідувальними структурами, гарантуючи узгодженість та результативність їх діяльності.

Національний координаційний центр кібербезпеки [105] є спеціальним робочим органом в структурі Ради національної безпеки і оборони України, робота котрого орієнтована на координування і виконання загального контролювання діяльності суб'єктів сфери безпеки й оборони, які задіяні в гарантуванні кібербезпеки держави. Центр здійснює функцію загального координатора національної системи реагування на кіберінциденти, кібератаки й кіберзагрози, гарантуючи узгодженість дій певних органів та структур. в рамках своїх повноважень Національний координаційний центр кібербезпеки здійснює підготовку і надає Раді національної безпеки і оборони України пропозиції стосовно введення кризового режиму в секторі кібербезпеки, і, крім того, координує виконання Стратегії кібербезпеки України. В той же час Центр задіяний у виробленні й уточненні стратегічних документів у згаданому секторі, в тому числі враховуючи положення Директиви ЄС стосовно мережевої, а також інформаційної безпеки (NIS 2). До того ж Центр встановлює основні пріоритети й концептуальні підходи щодо здійснення кібероперацій стратегічного рівня, виконує підготовку відповідних пропозицій Президентові України і гарантує координацію функціонування суб'єктів сфери безпеки й оборони у ході їх втілення. Значущим елементом функціонування Національного координаційного центру кібербезпеки вважається, крім того, узгодження стратегічних комунікацій в секторі кібербезпеки, що допомагає покращити дієвість державної політики в зазначеному аспекті.

Державна служба спеціального зв'язку та захисту інформації України [36] здійснює головні спеціальні функції, націлені на утворення і втілення державної політики у сфері кіберзахисту й технічного захисту даних. Вона гарантує нормативно-організаційну й практичну реалізацію заходів кіберзахисту державних інформаційних ресурсів, інформаційно-комунікаційних та електронних комунікаційних систем органів державної влади і, крім того, об'єктів критичної інформаційної інфраструктури. Вагома функція Державної служби спеціального зв'язку та захисту інформації – координація й налагодження реагування на кіберінциденти та кібератаки у рамках національної системи кібербезпеки, в тому числі за допомогою роботи урядової команди реагування на комп'ютерні надзвичайні події (CERT-UA). В зазначеному аспекті Державна служба спеціального зв'язку та захисту інформації гарантує здійснення моніторингу стану кіберзахисту, встановлення кіберзагроз, розгляд інцидентів і подання рекомендацій суб'єктам публічного управління стосовно зростання ступеня кіберстійкості. Державна служба спеціального зв'язку та захисту інформації, крім того, здійснює контрольні й наглядові функції, оцінюючи стан кіберзахисту, виконуючи аудит інформаційної безпеки й перевіряючи додержання визначених вимог в підпорядкованих і підзвітних структурах. Подібна діяльність – значущий елемент організаційного механізму забезпечення кібербезпеки, вона орієнтована на запобігання системним вразливостям в державній сфері. Окремим пунктом в роботі Державної служби спеціального зв'язку та захисту інформації є гарантування урядового й спеціального зв'язку, криптографічний та технічний захист даних, що відіграє критичну роль для сталої діяльності систем державного управління, насамперед на тлі воєнного стану й підвищених кіберзагроз.

Національна поліція України [103] здійснює правоохоронні й превентивні функції, націлені на протидію кіберзлочинності й захист прав та законних інтересів громадян, суспільства й держави в кіберпросторі. Вона – головний суб'єкт втілення державної політики в аспекті встановлення,

припинення, розслідування й розкриття кримінальних правопорушень, які мають зв'язок з застосуванням інформаційно-комунікаційних технологій. Головна функція Національної поліції у сфері кібербезпеки – боротьба з кіберзлочинністю, що охоплює протидію несанкціонованому доступу до інформаційних систем, розповсюдженню шкідливого програмного забезпечення, кібершахрайству, незаконному обігу персональної інформації й іншим злочинам в цифровій сфері. Здійснення зазначеної функції відбувається, в тому числі, за допомогою функціонування спеціальних підрозділів кіберполіції. В рамках організаційного механізму Національна поліція гарантує швидке реагування на кіберінциденти та кібератаки, виконує досудове розслідування, збирає та фіксує цифрові докази і, крім того, здійснює взаємодію з рештою суб'єктів національної системи кібербезпеки, правоохоронними й спеціальними органами. Значущим вектором функціонування Національної поліції є профілактика кіберправопорушень, яка втілюється за допомогою інформаційно-роз'яснювальних заходів, зростання ступеня цифрової і правової обізнаності громадян і, крім того, взаємодії із суб'єктами господарювання та громадянським суспільством.

Служба безпеки України [144] реалізує заходи щодо запобігання, встановлення, припинення й розкриття кримінальних правопорушень проти основ національної безпеки України, миру та безпеки людства і, крім того, кримінальних правопорушень терористичного спрямування, які скоюються в кіберпросторі чи із його застосуванням; виконує заходи контррозвідувального й оперативно-розшукового характеру, націлені на боротьбу із кібертероризмом, кібердиверсіями й кібершпигунством; здійснює координацію роботи суб'єктів гарантування кібербезпеки стосовно протидії кібершпигунству, кібертероризму, кібердиверсіям; конфіденційно здійснює перевірку готовності об'єктів критичної інфраструктури до потенційних кібератак і кіберінцидентів; протидіє кіберзлочинності, ефекти котрої здатні загрожувати життєво значущим інтересам держави; здійснює розслідування кіберінцидентів і кібератак стосовно державних електронних інформаційних

ресурсів, інформації, вимога стосовно захисту котрої визначена законом, критичної інформаційної інфраструктури; гарантує реагування на кіберінциденти, кібератаки й кіберзагрози в секторі державної безпеки.

Міністерство оборони України [99], Генеральний штаб Збройних Сил України виконують заходи щодо підготовки держави до відбиття воєнної агресії в кіберпросторі; реалізують військове співробітництво з НАТО, міжнародними організаціями й рештою суб'єктів оборонного сектора стосовно гарантування безпеки кіберпростору й спільного захисту від кіберзагроз.

Національний банк України [104] встановлює правила, вимоги й заходи, щоб забезпечити кіберзахист й інформаційну безпеку банків, інших учасників фінансових ринків, робота котрих регулюється і контролюється Національним банком, і, крім того, операторів платіжних систем, учасників платіжних систем й технологічних операторів платіжних послуг. Він контролює додержання цих вимог та гарантує роботу системи кіберзахисту для згаданих суб'єктів. З цією метою організовано Центр кіберзахисту Національного банку України, зокрема команду реагування на кіберінциденти, кібератаки й кіберзагрози. До того ж, НБУ здійснює організацію системи оцінки стану кіберзахисту, визначає вимоги стосовно виконання аудиту інформаційної безпеки й здійснює контроль їх реалізації, гарантуючи надійний захист фінансової інфраструктури України від кіберзагроз.

Міністерство закордонних справ України [98] допомагає зростанню євроінтеграційних процесів стосовно підходів, способів, інструментів забезпечення кібербезпеки, реалізації узгоджених з головними міжнародними партнерами заходів, націлених на зростання кіберстійкості України й зростання спроможностей національної системи кібербезпеки; гарантує координацію роботи стосовно співробітництва із міжнародними партнерами з метою спільної відповіді на кібератаки та усунення кризових випадків у кібербезпеці; гарантує активну участь України в роботі міжнародних організацій стосовно спільного формування норм поведінки в кіберпросторі й

покращення належної міжнародної нормативно-правової основи; допомагає реалізації спільних з Євросоюзом заходів, націлених на зростання стійкості у кіберпросторі й здатності здійснювати розслідування та переслідування кіберзлочинності і реагувати на кіберзагрози; виконує координацію процедури введення гармонізованого з євроатлантичною спільнотою підходу до впровадження санкцій у відповідь на підривні дії в кіберпросторі, узгодження із міжнародними партнерами процедури спільних дипломатичних дій та заходів у відповідь на деструктивну кіберактивність; здійснює інші завдання згідно із законом.

Реалізація організаційно-технічної моделі кіберзахисту, що вважається складовою національної системи кібербезпеки, виконується Державним центром кіберзахисту [37]. Центр здійснює системні навчання щодо питань кіберзахисту і в співробітництві з рештою суб'єктів забезпечення кібербезпеки напрацьовує алгоритми реагування на кіберзагрози, заходи протидії подібним загрозам і, крім того, програми й способи реалізації кібернавчань. Також Державний центр кіберзахисту оцінює стан кіберзахисту інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем органів державної влади, державних органів, органів місцевого самоврядування і, крім того, об'єктів критичної інфраструктури й критичної інформаційної інфраструктури.

В органах державної влади, які є власниками чи розпорядниками інформаційних, електронних комунікаційних й інформаційно-комунікаційних систем, у котрих здійснюється обробка державних інформаційних ресурсів чи службових даних й інформації, яка є державною таємницею, формуються підрозділи з кіберзахисту і призначаються керівники з кіберзахисту, котрим прямо підпорядковуються такі підрозділи, а в органах місцевого самоврядування – особи, котрі здійснюють їх завдання і функції.

Органи державної влади, військові формування, сформовані згідно з законами України, державні підприємства, установи й організації для ліквідації ймовірних наслідків кіберінцидентів і кібератак роблять резервні

копії національних електронних інформаційних ресурсів, які знаходяться в їхньому володінні чи розпорядженні і вважаються критичними для їхнього стабільного функціонування, і виконують їх передачу на зберігання до Національного центру резервування державних інформаційних ресурсів, окрім тих, передавання котрих обмежено законодавством. Алгоритм передавання, збереження й доступу до згаданих копій встановлюється Кабінетом Міністрів України. Національним центром резервування державних інформаційних ресурсів забезпечується:

1) «безперервність роботи відповідного національного електронного інформаційного ресурсу, резервного копіювання інформації та відомостей національного електронного інформаційного ресурсу через єдині основний та резервний захищені центри обробки даних (дата-центри), призначені для обробки національних електронних інформаційних ресурсів, резервного копіювання національних електронних інформаційних ресурсів;

2) надійне функціонування серверного обладнання, системи зберігання даних, активного мережевого обладнання, архітектурно-технічних рішень щодо резервного копіювання й дублювання інформаційних систем, постійно працюючої інженерної інфраструктури;

3) здійснення обов’язкового контролю за статистичними даними роботи з фізичного захисту об’єктів, системи управління та моніторингу інформаційних систем, комплексу організаційних заходів;

4) переміщення протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування резервних копій національних електронних інформаційних ресурсів до електронних комунікаційних мереж закордонних дипломатичних установ України в порядку, встановленому Кабінетом Міністрів України.

5. Розроблення та застосування платних, безоплатних умов пошуку та/або виявлення потенційних вразливостей в інформаційно-комунікаційних системах, в яких обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, а

також на об’єктах критичної інформаційної інфраструктури здійснюються відповідно до порядку пошуку та/або виявлення потенційних вразливостей, встановленого Кабінетом Міністрів України» [129].

В Україні формується й гарантується функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози стосовно інформаційних, електронних комунікаційних, а також інформаційно-комунікаційних систем, де відбувається обробка державних інформаційних ресурсів чи інформації з обмеженим доступом, вимога стосовно захисту котрої визначена законом, об’єктів критичної інформаційної інфраструктури. У даному контексті уповноваженим органом, який створює належні умови для функціонування національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, є Державна служба спеціального зв’язку та захисту інформації України. Склад національної системи реагування на кіберінциденти, кібератаки, кіберзагрози включає:

1) CERT-UA – національна команда реагування на кіберінциденти, кібератаки, кіберзагрози (національний CSIRT), діяльність якої забезпечується Державною службою спеціального зв’язку та захисту інформації України

2) галузеві та регіональні команди реагування на кіберінциденти, кібератаки, кіберзагрози (далі – галузеві, регіональні CSIRT) – створюються органами державної влади або органами місцевого самоврядування з метою посилення спроможності національної системи реагування на кіберінциденти, кібератаки, кіберзагрози у відповідній галузі, сфері або відповідному регіоні з урахуванням вимог до організаційно-технічної спроможності, встановлених Державною службою спеціального зв’язку та захисту інформації України, та взаємодіють з правоохоронними, розвідувальними та контррозвідувальними органами, суб’єктами оперативно-розшукової діяльності, іншими суб’єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України.

3) Національна поліція України, Служба безпеки України – взаємодіють у рамках національної системи реагування на кіберінциденти, кібератаки,

кіберзагрози з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози в порядку, встановленому Кабінетом Міністрів України, з урахуванням вимог цього Закону та в межах повноважень, визначених законом.

4) приватні команди реагування – можуть залучатися для надання операторам критичної інфраструктури, власникам або розпорядникам критичної інформаційної інфраструктури, органам державної влади та органам місцевого самоврядування окремих послуг, пов'язаних з реагуванням на кіберінциденти, виконання окремих завдань галузевих, регіональних CSIRT, а також взаємодіяти з іншими суб'єктами національної системи реагування на кіберінциденти, кібератаки, кіберзагрози, у тому числі щодо обміну інформацією про кіберінциденти, кібератаки, кіберзагрози, за умови організаційно-технічної спроможності та в порядку, встановленому Державною службою спеціального зв'язку та захисту інформації України.

5) Національний координаційний центр кібербезпеки – здійснює загальну координацію функціонування суб'єктів національної системи реагування на кіберінциденти, кібератаки, кіберзагрози» [129].

Щоб гарантувати скоординоване, оперативне й ефективне реагування на кризову ситуацію через кіберінцидент, кібератаку, кіберзагрозу в складі Національного координаційного центру кібербезпеки утворюється та провадить діяльність регулярно діюча Об'єднана група реагування на кіберінциденти, кібератаки, кіберзагрози.

Варто зауважити, що існує ряд проблем організаційного забезпечення публічного управління у сфері забезпечення кібербезпеки України, які можна узагальнити так:

1. Нечітка структура і розподіл повноважень. Наявна розмитість компетенцій між центральними органами влади, підрозділами сфери безпеки й оборони, а також органами місцевого самоврядування, через що ускладнюється оперативне ухвалення рішень та взаємодія у разі кіберінцидентів.

2. Фрагментарність координації між суб’єктами кібербезпеки. Неіснування єдиної централізованої системи координації й узгоджених механізмів взаємодії між державними органами, правоохоронними структурами, приватним сектором та громадською сферою спричиняє дублювання функцій і зменшення результативності управлінських рішень.

3. Недостатнє кадрове забезпечення та брак висококваліфікованих фахівців. Підрозділи кібербезпеки нерідко мають справу із браком фахівців у секторі інформаційної безпеки, цифрової криміналістики й кібероперацій, з огляду на що обмежуються змоги системного реагування на кібератаки.

4. Обмежені ресурси та технологічна відсталість. В органів публічного управління є не завжди новітні технологічні інструменти, програмне забезпечення, а також інфраструктура для вчасного встановлення й усунення кіберзагроз.

5. Незадовільна інтеграція стратегічного планування та управлінських процедур. Неіснування узгоджених механізмів планування, оцінювання ризиків та реагування на кіберзагрози робить більш складними швидке ухвалення рішень і реалізацію результативних запобіжних заходів.

6. Недостатня регіональна представленість та взаємодія з місцевим рівнем. Органи місцевого самоврядування нерідко не включають в єдину систему реагування на кіберінциденти, через що ослаблюється загальний ступінь кіберстійкості держави.

7. Слабка міжвідомча та міжнародна взаємодія. Відсутність дієвих механізмів обміну даними й координації дій із міжнародними партнерами, а також іншими відомствами стає на заваді вчасному реагуванню на кібератаки й загрози стратегічного плану.

Отже, наявні проблеми організаційного забезпечення публічного управління у сфері кібербезпеки України вказують на потребу системного покращення управлінських механізмів, збільшення координації між суб’єктами кібербезпеки, зростання кадрових ресурсів і модернізації технологічної інфраструктури. Усунення згаданих викликів дасть можливість

покращити результативність реагування на кіберзагрози, посилити стійкість національної системи кібербезпеки й гарантувати відповідний ступінь захисту державних інтересів, критичної інфраструктури, а також інформаційних ресурсів України на тлі кіберризиків, які зростають.

Що стосується *інформаційно-технічного забезпечення*, варто зауважити, що це сукупність інформаційних ресурсів, технічних засобів, цифрових технологій, програмно-апаратних комплексів та організаційних процедур, які забезпечують збирання, обробку, зберігання, аналіз і захист інформації, необхідної для ухвалення та реалізації управлінських рішень у сфері кібербезпеки.

Інформаційно-технічне забезпечення допомагає швидкості, обґрунтованості й координації управлінських дій суб'єктів публічної влади, гарантує інформаційну взаємодію між ними і, крім того, посилює ступінь кіберстійкості державних інформаційних систем та об'єктів критичної інфраструктури.

Варто зауважити, що Постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426 затверджено Положення про організаційно-технічну модель кіберзахисту [118]. Цим Положенням визначається порядок забезпечення реалізації організаційно-технічної моделі кіберзахисту. Організаційно-технічна модель кіберзахисту є «комплексом заходів, сил і засобів кіберзахисту, спрямованих на оперативне (кризове) реагування на кібератаки та кіберінциденти, впровадження контрзаходів, спрямованих на мінімізацію вразливостей комунікаційних систем. Організаційно-технічна модель кіберзахисту складається з організаційно-керуючої, технологічної та базисної інфраструктури кіберзахисту та впроваджується для забезпечення функціонування національної системи кібербезпеки» [118]. Зважаючи на подане вище, можливо зрозуміти, що організаційно-технічна модель кіберзахисту є такою моделлю, що допоможе консолідувати зусилля суб'єктів гарантування кібербезпеки й сформувати передумови для безпечного функціонування кіберпростору, його застосування на користь людини,

соціуму та держави, в тому числі шляхом проведення заходів, націлених на захист національних інформаційних ресурсів, кіберзахист об'єктів критичної інформаційної інфраструктури, гарантування їхньої кіберстійкості, сталого функціонування інформаційної інфраструктури державної, а також приватної галузі економіки.

Зауважимо, що «технологічна інфраструктура формується мережею взаємодіючих технічних підрозділів кіберзахисту (CSIRTів), засобів та сервісів (служб) кіберзахисту, інформаційних систем взаємодії та обміну інформацією про кіберінциденти, кібератаки та кіберзагрози, Операційних центрів кібербезпеки (Security Operations Centers) та інших організаційно-технічних об'єктів, що забезпечують реалізацію функцій та процесів кіберзахисту в межах політик (механізмів, процедур), визначених суб'єктами кіберзахисту» [102]. У контексті публічного управління інформаційно-технічне забезпечення виконує функцію інфраструктурної основи національної системи кібербезпеки та охоплює:

– комплекс державних інформаційних ресурсів, реєстрів, баз даних і систем моніторингу кіберзагроз;

– сукупність інформаційно-комунікаційних та електронних комунікаційних систем органів державної влади і органів місцевого самоврядування;

– ряд спеціалізованих технічних засобів, за допомогою яких виявляють, аналізують та реагують на кіберінциденти і кібератаки (CERT/CSIRT-системи, центри кіберзахисту);

– комплекс засобів криптографічного та технічного захисту інформації, систем резервування й відновлення даних;

– ряд програмно-аналітичних інструментів підтримки управлінських рішень, оцінювання ризиків і прогнозування кіберзагроз.

До засобів кіберзахисту, що застосовуються з метою введення організаційно-технічної моделі кіберзахисту, належать системи встановлення вразливостей та реагування на кіберінциденти й кібератаки, інформаційні

технології, технічні та програмні засоби (прилади, устаткування, комплекси), що застосовуються для гарантування кіберзахисту національних електронних інформаційних ресурсів, а також об'єктів кіберзахисту. Заходами з кіберзахисту, що реалізуються в ході введення організаційно-технічної моделі кіберзахисту, вважаються організаційні, правові, інженерно-технічні заходи, заходи, якими забезпечується криптографічний та технічний захист інформації, що реалізуються силами кіберзахисту й основуються на засадах особистої відповідальності за свої дії, а також колективної відповідальності за безпеку кожного, гарантування пропорційності та/чи співрозмірності заходів фактичним і ймовірним ризикам.

В межах введення організаційно-технічної моделі кіберзахисту сили кіберзахисту в рамках своєї компетенції реалізують базові заходи із кіберзахисту, зокрема стосовно вивчення результативності й корегування проведених заходів із кіберзахисту, затвердження планів кіберзахисту і планів реагування на кіберінциденти/кібератаки. До базових заходів кіберзахисту відноситься ряд заходів щодо:

– «управління – визначення стратегій, політик, ролей та обов'язків, здійснення моніторингу щодо управління ризиками у сфері кібербезпеки;

– ідентифікації – оцінка реальних та потенційних ризиків у сфері кібербезпеки для запобігання та нейтралізації кіберзагроз;

– забезпечення захисту – розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталого та надійного функціонування об'єктів кіберзахисту, удосконалення систем реагування на кіберінциденти та кібератаки з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

– виявлення – проведення ідентифікації, збору та обробки кіберінцидентів/кібератак;

– реагування – запобігання кіберінцидентам та кібератакам, належне інформування про них, запобігання негативним наслідкам, їх мінімізація та усунення;

– відновлення – поновлення штатного режиму функціонування об’єктів кіберзахисту після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки та кіберінциденту» [118].

Зауважимо, що здійснення заходів з кіберзахисту системами кіберзахисту передбачає:

– «ідентифікацію – виявлення реальних і потенційних кіберзагроз для запобігання їм і їх нейтралізації.

– захист – розроблення та впровадження методів, засобів, процедур кіберзахисту, спрямованих на забезпечення сталості і надійності функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних та технологічних систем.

– виявлення – проведення моніторингу визначення, збору та обробки нетипових подій у кіберпросторі.

– реагування – вжиття заходів, спрямованих на запобігання кіберінцидентам, кібератакам, мінімізації їх можливих наслідків (запобігання виникненню загроз життю або здоров’ю людей та заподіяння шкоди майну), удосконалення систем кіберзахисту, з урахуванням необхідності забезпечення пропорційності та/або співрозмірності можливостей таких систем реальним та потенційним ризикам;

– відновлення – поновлення штатного режиму функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних, технологічних систем після кібератаки, відновлення інформації та відомостей у разі їх пошкодження або видалення, створення умов для проведення розслідування кібератаки» [102].

Для того, щоб технологічна інфраструктура функціонувала ефективно, суб’єктами кіберзахисту:

– реалізують заходи щодо швидкого й дієвого захисту кіберпростору стосовно мінімізації ризиків у секторі кібербезпеки, протидії кібератакам, кіберзлочинам, кібертероризму, кібершпигунству та, крім того, гарантування кібероборони й кіберрозвідки через збір, розгляд, оцінку, узагальнення й розповсюдження даних про ризики в секторі кібербезпеки, кіберінциденти, кібератаки;

– реалізують заходи з оперативного (кризового) реагування на кібератаки й кіберінциденти, в тому числі через системи інформаційного обміну стосовно таких подій, контрзаходи, націлені на ліквідацію вразливостей об’єктів кіберзахисту;

– реалізують заходи з кіберзахисту об’єктів кіберзахисту, у котрих здійснюється опрацювання національних електронних інформаційних ресурсів та/чи котрі застосовуються державними органами, органами місцевого самоврядування, військовими формуваннями, утвореними згідно із законом;

– гарантують діяльність систем реагування на кіберінциденти й кібератаки стосовно об’єктів кіберзахисту;

– здійснюють розвиток об’єднання (мережі) команд реагування на комп’ютерні надзвичайні події, здійснюють взаємодію із командами реагування на комп’ютерні надзвичайні події та, крім того, підприємствами, установами й організаціями, незважаючи на форму власності, котрі здійснюють діяльність, яка має зв’язок з гарантуванням безпеки у кіберпросторі;

– взаємодіють між собою згідно з рішеннями суб’єктів гарантування кібербезпеки;

– надають інформацію про кібератаки/кіберінциденти і вірогідні ризики в секторі кібербезпеки інші сили кіберзахисту й суб’єктів гарантування кібербезпеки, обробляють одержані від них, в тому числі від громадян, дані про кіберінциденти й стосовно об’єктів кіберзахисту, забезпечують консультативну й практичну допомогу щодо питань реагування на кібератаки;

– допомагають державним органам, органам місцевого самоврядування, військовим формуванням, сформованим згідно із законом, підприємствам, установам і організаціям незалежно від форми власності і, крім того, громадянам в розв'язанні питань стосовно кіберзахисту і протидії кіберзагрозам;

– формують і гарантують діяльність головних елементів системи захищеного доступу державних органів до інтернету, системи антивірусного захисту національних електронних інформаційних ресурсів;

– задіяні в реалізації кібернавчань, напрацюванні програм і технологій їх здійснення, алгоритмів реагування на кіберзагрози і здійснюють заходи стосовно протидії кіберзагрозам, з кібергігієни;

– одержують та надають послуги із кіберзахисту.

При цьому, варто зауважити, що у ході реалізації базисної інфраструктури кіберзахисту забезпечується:

– «захист у кіберпросторі національних електронних інформаційних ресурсів, що обробляються на об'єктах кіберзахисту;

– захист об'єктів кіберзахисту, у тому числі шляхом здійснення базових заходів з кіберзахисту;

– захист інтересів громадянина та суспільства у кіберпросторі;

– розроблення програм розвитку основ кібергігієни на національному, галузевому (регіональному, місцевому), об'єктовому рівні;

– здійснення заходів з формування культури кібербезпеки суб'єктами забезпечення кібербезпеки;

– інформування громадян про кіберінциденти» [118].

Базисна інфраструктура кіберзахисту функціонує, щоб гарантувати захист життєво значущих інтересів людини та громадянина, суспільства й держави, національних інтересів у кіберпросторі.

Зауважимо, що проблеми інформаційно-технічного забезпечення публічного управління у сфері забезпечення кібербезпеки характеризуються

системним характером, що розкривається у технологічних та управлінських чинниках. Зокрема:

1. Зношеність та фрагментарність інформаційно-технічної інфраструктури. Застарілість значної частини інформаційно-комунікаційних систем, що функціонують в органах публічної влади, у зв'язку з чим знижується їх кіберстійкість та ускладнюється інтеграція з сучасними системами кіберзахисту.

2. Відсутність єдиних технічних стандартів і протоколів взаємодії. Наявність несумісності між програмно-апаратними рішеннями, які використовують різні органи влади, у зв'язку з чим ускладнюється інформаційний обмін, здійснення централізованого моніторингу кіберзагроз у координація реагування.

3. Недостатній рівень автоматизації процесів управління кібербезпекою. Збір, аналіз та обробка інформації про здійснення кіберінцидентів здійснюється ручним або напівавтоматизованим способом, що здійснює негативний вплив на тривалість прийняття ефективних управлінських рішень.

4. Обмежені можливості моніторингу та прогнозування кіберзагроз. Інформаційно-аналітичні системи не завжди супроводжуються комплексним аналізом великих масивів даних, кореляцією подій і прогнозування розвитку кіберзагроз у режимі реального часу.

5. Недостатній рівень захисту державних інформаційних ресурсів. Фрагментарність обладнаності державних інформаційних систем сучасними криптографічними та технічними засобами захисту інформації, здійснення резервних копій та відновлення даних, чим підвищується ризик втрати або компрометації інформації.

6. Проблеми інтеграції хмарних технологій та нових цифрових рішень. Недостатність врегулювання технічних механізмів при використанні хмарних сервісів в органах публічного управління, що провокує виникнення додаткових кіберризиків.

7. Слабка інтеграція інформаційно-технічного забезпечення з управлінськими процесами. Недостатність використання інформаційних систем для того, щоб підтримувати стратегічне та оперативне управління кібербезпекою.

Ряд перелічених проблем знижує ефективність публічного управління у сфері забезпечення кібербезпеки України та актуалізує потребу системної модернізації інформаційно-технічного забезпечення, враховуючи сучасні безпекові виклики і міжнародний досвід.

Проведений аналіз нормативно-правового, організаційного та інформаційно-технічного забезпечення публічного управління у сфері забезпечення кібербезпеки України свідчить про утворення комплексної, багатоступеневої системи державного реагування на новітні кіберзагрози. Нормативно-правове забезпечення започатковує базові принципи державної політики в секторі кібербезпеки, встановлює коло суб'єктів, їх повноваження і процеси взаємодії і, крім того, гарантує інтеграцію національного законодавства з міжнародними і європейськими стандартами. Організаційне забезпечення публічного управління у сфері кібербезпеки основується на функціонуванні системи спеціальних державних органів і координаційних інституцій, що гарантують стратегічне планування, міжвідомчу співдію і реагування на кіберінциденти. Інформаційно-технічне забезпечення є інфраструктурним базисом публічного управління в секторі кібербезпеки, гарантуючи діяльність державних інформаційних систем, здійснення моніторингу кіберзагроз, захист інформаційних ресурсів та сприяння управлінським рішенням.

Підвищення ефективності публічного управління у сфері забезпечення кібербезпеки України є можливим при умові докладання узгоджених зусиль розвитку нормативно-правових, організаційних та інформаційно-технічних механізмів, їх системного впровадження й спрямування на довгострокове посилення національної безпеки на фоні зростаючих кіберризиків та цифрової трансформації суспільства.

2.2. Особливості реалізації публічного управління у сфері забезпечення кібербезпеки України в умовах правового режиму воєнного стану

В Україні протягом останніх декількох років питання кібербезпеки стали на рівні національного пріоритету – зазнаючи впливу як безперервних гібридних і кібератак в період війни, так і динамічної цифрової трансформації публічної сфери. Конфлікт з російським агресором істотно посилив загрози у кіберпросторі, що спонукало державу пришвидшити формування єдиних механізмів захисту критичної інфраструктури, систем реагування і координації між відомствами.

Сучасний стан публічного управління у сфері забезпечення кібербезпеки України відзначається активним розвитком інституцій та нормативів, зазнаючи тиску реальних загроз, в той же час супроводжується викликами втілення (координація, потенціал, стандартизація). Зазначений баланс між досягненнями і нерозв’язаними проблемами формує основні вектори наступних наукових досліджень і практичних реформ у сфері публічного управління кібербезпекою.

В нинішньому цифровому світі питання кібербезпеки набуває дедалі більшої актуальності, насамперед для України, котра не тільки розвиває свою ІТ-сферу, а також здійснює боротьбу в кіберпросторі. Протягом останніх декількох років кіберзагрози сягнули нових масштабів, ставлячи вимогу зростання захисту як на рівні держави, так і в приватному секторі.

Варто звернути увагу, що із червня 2022 року бізнес України стикається із безпрецедентним зростанням числа кібератак. З-поміж головних цілей – телеком, державні інформаційні ресурси, енергетика, фінанси, промисловість. В кожного клієнта існують своєрідні потреби з огляду на характер діяльності й певні загрози:

1. «Фінанси. Пріоритетами є захист даних, безпека транзакцій, дотримання галузевих стандартів (наприклад, PCI DSS) та надійність захисту від шахрайства, фішингу та атак з вимогою викупу.

2. Телеком. Пріоритетами є захист мережевої інфраструктури, запобігання DDoS-атакам, захист даних.

3. Промисловість. Пріоритетами є захист промислових систем управління (ПСУ) і забезпечити безперервності бізнес-процесів.

4. Держава. Пріоритетами є побудова та модернізації систем захисту, в яких обробляються державні інформаційні ресурси, в тому числі, інформація з обмеженим доступом, організаційні та технічні заходи кіберзахисту критичної інформаційної інфраструктури, вдосконалення нормативних документів для запровадження кращих практик.

5. Енергетика. Пріоритетами є захист енергосистем і ланцюгів енергопостачання, безпека операційних технологій» [106].

Зважаючи на це, варто зауважити, що рівень ухилення країн від кіберзагроз вимірюється Національним індексом кібербезпеки (NCSI), який запропонувала проєктна група в Академії електронного урядування в Таллінні [75]. NCSI сконцентровується на факторах кібербезпеки, які визначає і втілює центральний уряд відповідно до чотирьох груп інформації, що презентують: чинну законодавчу основу – нормативно-правові документи, положення, накази та інше; утворені підрозділи, які забезпечують кібербезпеку, – існуючі організації, відділи та ін.; моделі співробітництва – комітети, робочі групи та ін.; результати – політику, вправи, технології, вебсайти, програми тощо. Оцінка NCSI показує, який відсоток одержала держава, порівнюючи з найбільшими даними. Якнайбільше значення NCSI – у всіх випадках 100 (100 відсотків).

Динаміку нашої країни за показником NCSI у порівнянні з іншими 160 країнами світу розглянемо на рис. 2.1.

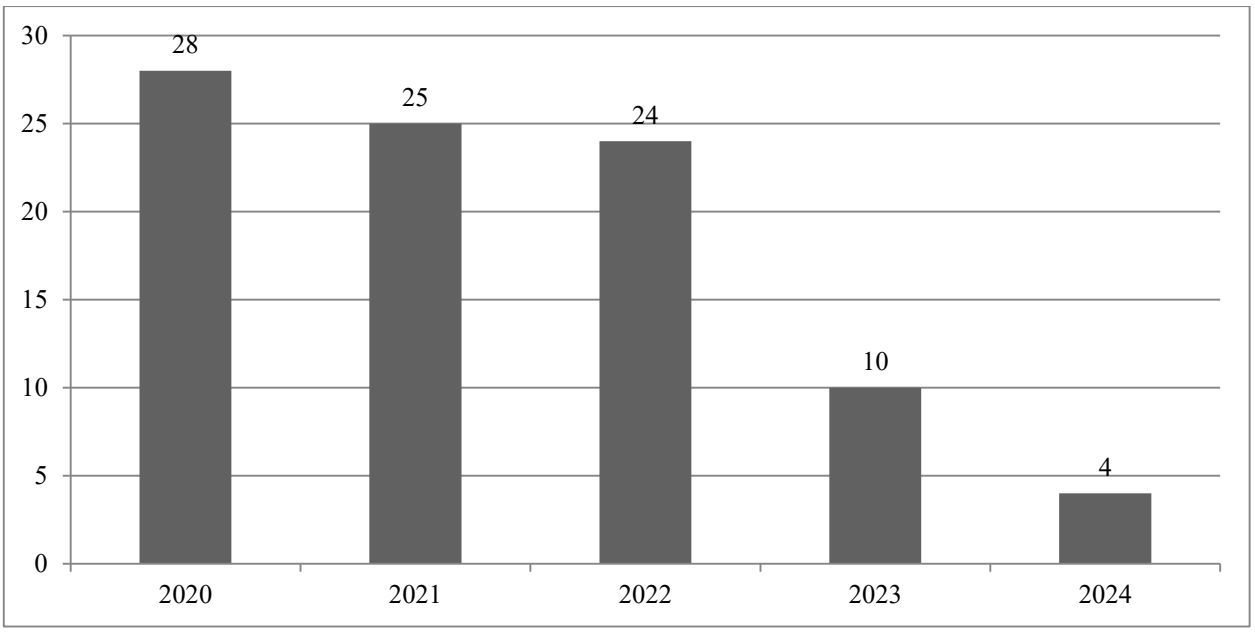

Рис. 2.1. Рейтинг України за Національним індексом кібербезпеки (NCSI) у 2020-2024 рр.

Джерело: розраховано за матеріалами [195]

Як бачимо, значення показників України у світовому рейтингу кібербезпеки динамічно поліпшуються, що спричинене цілеспрямованою політикою держави, тим, що держава пристосовується до умови, коли відбувається гібридна війна, й здійснює активний розвиток цифрової інфраструктури. Зазначеним поліпшенням показників стверджується, що держава стає значно стійкішою до кіберзагроз, що націлені ззовні, й спроможна захищати національний інформаційний простір.

Зауважимо, що «український ринок кібербезпеки зріс у чотири рази за останні вісім років і у 2024 році становить $138 млн. За прогнозами, ринок зросте ще на 50% протягом п’яти років і досягне $209 млн. Ключовий сегмент українського ринку кібербезпеки – мережева безпека» [153], див. рис. 2.2. В 2016-2024 рр. масштаби українського ринку кібербезпеки засвідчували стабільний і динамічний розвиток – із 32 млн. дол. США у 2016 році до 138 млн. дол. США у 2024 р., іншими словами, зросли більше ніж вчетверо. Така позитивна динаміка показує поступове розуміння кібербезпеки як однієї з головних складових національної безпеки й публічного управління.

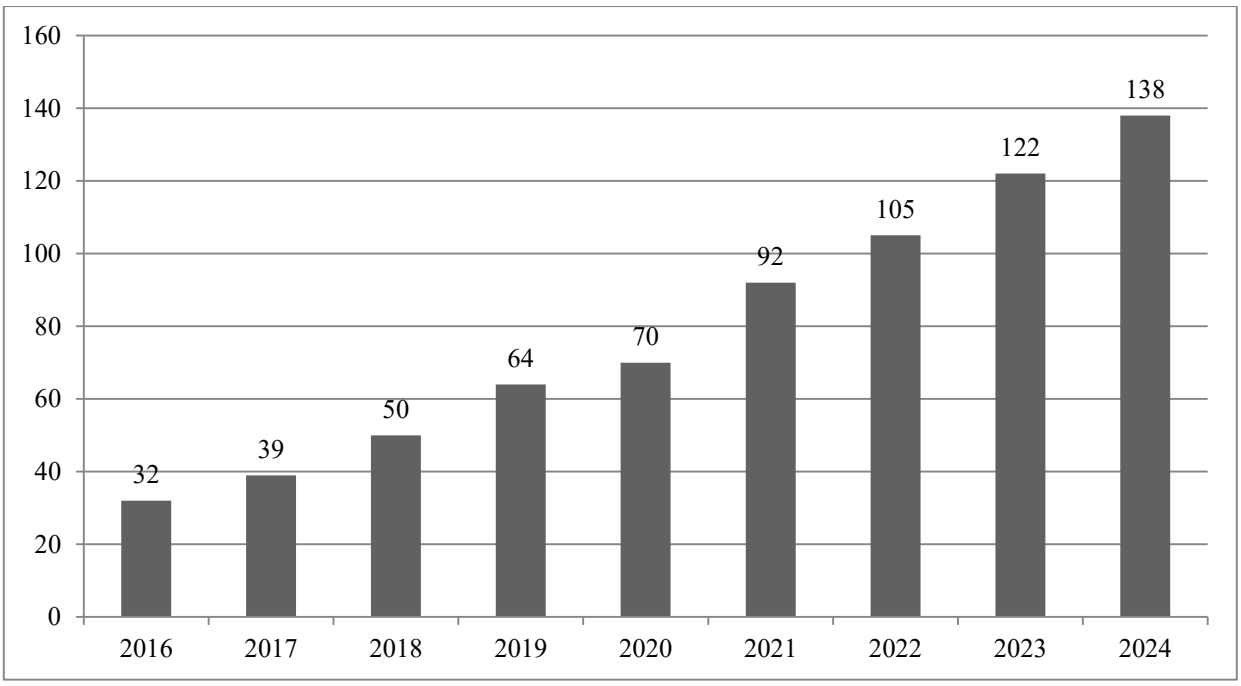

Рис. 2.2. Обсяг українського ринку кібербезпеки 2016-2024 рр., млн. доларів США

Джерело: розраховано за матеріалами [106]

Максимальні темпи збільшення простежувалися в період 2017-2019 й 2020-2021 рр., що має зв'язок із активізацією цифрової трансформації державної сфери, введенням електронних сервісів та збільшенням числа кібератак на органи влади й об'єкти критичної інфраструктури. Деяке гальмування темпів у 2020 р. можливо обґрунтувати впливом коронавірусної пандемії, проте вже із 2021-го ринок знову увійшов у стадію пришвидшеного зростання, що продовжив зберігатися також після початку повномасштабної війни у 2022 р. В цілому збільшення ринку кібербезпеки віддзеркалює реальну потребу держави й бізнесу щодо зростання захисту інформаційних систем на тлі воєнних, гібридних та цифрових загроз та, крім того, засвідчує стратегічну значущість згаданого сектора для системи публічного управління України на сучасному етапі.

Було здійснено перерозподіл ресурсів для підтримки віддаленої роботи, що спричинило зменшення витрат на передові рішення із кібербезпеки. Максимальне збільшення прослідковувалося в секторі хмарної безпеки (+76%), тому що компанії дедалі більше покладалися на хмарні сервіси для

віддаленої роботи. Пришвидшення зростання ринку в 2021 р. було спричинене збільшенням кіберзлочинності, зростанням уваги до кібербезпеки й постійною діловою активністю шляхом реструктуризації в обставинах карантину. Помірне зростання ринку в 2022 р. було спричинене ревокаціями компаній і закриттями офісів, що обумовили мінімізацію внутрішнього попиту на кібербезпеку і гальмування збільшення інвестицій. Державою почасти задовольнялися запити в секторі кібербезпеки завдяки працівникам державного сектору й мобілізації. На рис. 2.3 наведено динаміку обсягів допомоги США Україні в кібербезпеці за 2016-2024 роках.

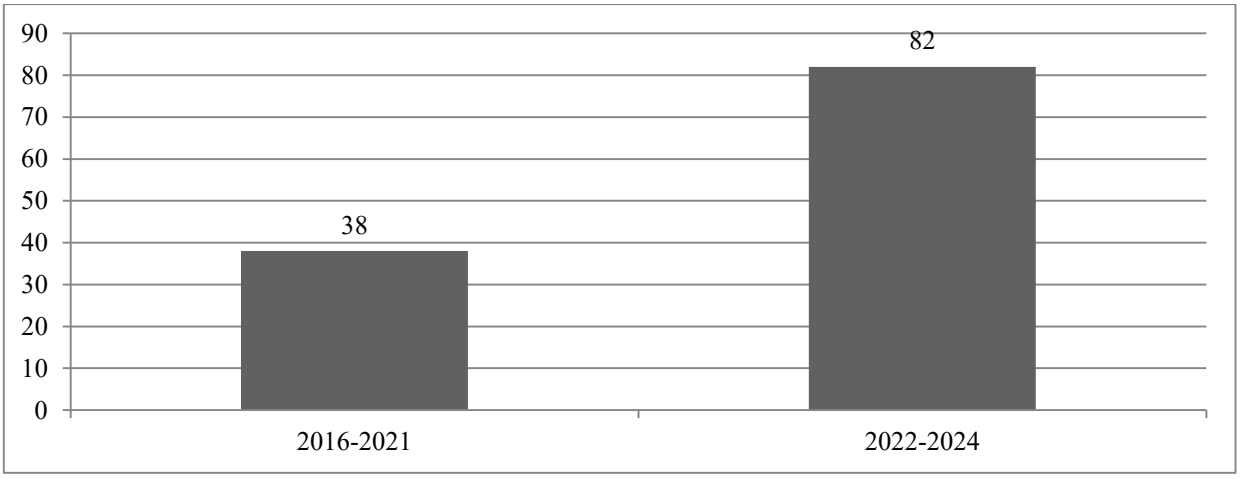

Рис. 2.3. Допомога США Україні в кібербезпеці за 2016-2024, млн. доларів США

Джерело: розраховано за матеріалами [106]

Протягом 2016-2024 рр. допомога США Україні в секторі кібербезпеки значно збільшилася, що чітко прослідковується під час порівняння двох часових періодів. Коли в 2016-2021 рр. загальний обсяг фінансової допомоги складав 38 млн. дол. США, то вже у 2022-2024 роках він збільшився до 82 млн. дол. США, іншими словами, більше аніж в два рази. Такий динамічний розвиток вказує на різке зростання уваги США до кіберстійкості України після початку повномасштабної збройної агресії рф, коли кіберпростір став одним із головних фронтів гібридної війни. Зростання масштабів допомоги виражає розуміння стратегічної значущості захисту державних інформаційних ресурсів, об’єктів критичної інфраструктури і систем публічного управління від кібератак. У той же час це засвідчує трансформацію кібербезпеки з

допоміжного вектора міжнародної підтримки в головну складову безпекового співробітництва між Україною, а також її стратегічними партнерами.

Українська екосистема кібербезпеки знаходиться на етапі утворення. На цій фазі можливо виокремити такі характерні ознаки:

1. «Партнерством між державою, бізнесом та міжнародними структурами. приватний сектор взаємодіє з державою (наприклад Держспецзв'язку, НБУ, НКЦК, СБУ, МОУ) та міжнародними структурами для спільного моніторингу загроз, реагування, навчання. обміну даними.

2. Закритістю спільноти. вітчизняний ринок кібербезпеки видається ще більш закритим та ізольований за світовий, що робить вихід на нього складним для нових гравців та стартапів.

3. Значний практичний досвід. українські фахівці з кібербезпеки мають виняткову експертизу в захисті від DDoS-атак та інших видів кібератак, сформовану завдяки великому досвіду реагування на російську кіберагресію. Їхній практичний досвід захисту критичної інфраструктури вигідно відрізняє їх від регіональних конкурентів» [106].

У даному контексті варто зауважити, що основними рушійними силами ринку в Україні є:

1. «Всебічна цифровізація. У міру того, як бізнес та уряд впроваджують цифрові рішення, вони стикаються з підвищеним ризиком кіберзагроз, що вимагає посилення заходів кібербезпеки для захисту конфіденційних даних та забезпечення безперебійної роботи.

2. Ріст обсягу кібератак. Фактичне перебування у стані кібервійниє основною причиною збільшення кількості кібератак. Організації в усіх секторах стикаються з підвищеними ризиками для своєї діяльності та безпеки даних, що змушує інвестувати в передові рішення з кібербезпеки.

3. Зростання ризику реальних втрат. Кібератаки, такі як віруси-вимагачі, витоки даних порушують бізнес-діяльність, призводять до простоїв, і часто вимагають значних витрат на відновлення. Окрім фінансових збитків,

компанії можуть зіткнутись зі зниженням доходів, репутаційними збитками та втратою довіри клієнтів.

4. Стимулювання ринку донорами. Під час повномасштабної агресії розвиток галузі значною мірою залежить від фінансування за рахунок МТД (наприклад, проекти USAID) або прямої підтримки світовими та національними компаніями. Їх підтримка залишається критично важливою в умовах обмеженої участі держави.

5. Ріст популярності штучного інтелекту. Зростання спроможностей продуктів ШІ створює можливості для здійснення кібератак нової потужності та інтенсивності і використовується для посилення заходів безпеки, дозволяючи швидше виявляти загрози, аналізувати дані і автоматизувати механізми захисту» [153; 106].

Таким чином, зазначені чинники утворюють сталий попит на сучасні рішення в секторі кіберзахисту і спричиняють структурні зміни на ринку кібербезпеки України. Зростання цифровізації, посилення інтенсивності кібератак та ризиків фактичних втрат і, крім того, активне сприяння зі сторони міжнародних донорів та введення технологій штучного інтелекту не тільки прискорюють загальне зростання ринку, а також встановлюють головні вектори його зростання. В зазначеному аспекті насамперед показовим вважається сектор хмарної безпеки, котрий найчутливіше реагує на трансформацію цифрового простору й необхідність у захисті розподілених інформаційних ресурсів, що засвідчується його інтенсивним збільшенням під час повномасштабної війни. За час повномасштабного вторгнення ринок хмарної безпеки виріс втричі до 1,7 млн. доларів (див. рис. 2.4).

З огляду на можливість пошкодження сервісів і систем при російському вторгненні компанії стали переносити ІТ-інфраструктури у хмарні сервіси. Після того, як розпочалося вторгнення рф, Національний банк України дав дозвіл фінустановам здійснити перенесення даних і систем за межі держави, що посилило попит на хмарні сервіси.

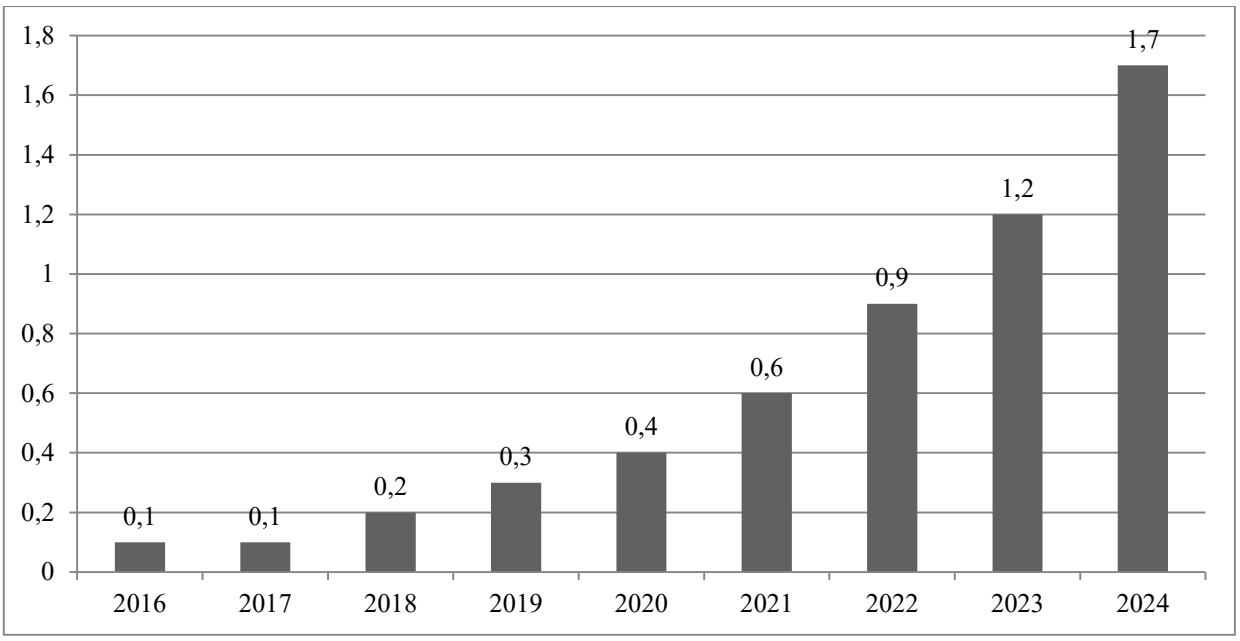

Рис. 2.4. Обсяг ринку хмарної безпеки в Україні 2016-2024, млн. доларів США

Джерело: розраховано за матеріалами [106]

Поточний обсяг ринку хмарної безпеки не бере до уваги значну кількість рішень, що надають державним органам безоплатно у межах міжнародної технічної підтримки. По завершенню військових дій і після скорочення масштабів міжнародної технічної допомоги державні органи здійснять перехід на оплату цих послуг, що спричинить збільшення загального обсягу ринку хмарної безпеки.

В комплексі зазначені умови вказують на те, що зростання хмарних технологій і належних інструментів захисту в Україні володіє не тільки ситуативним, а також довгостроковим характером. Масове перенесення IT-інфраструктури у хмарні середовища, нормативні послаблення зі сторони регуляторів і велике значення міжнародної технічної підтримки утворили нову конфігурацію ризиків у кіберпросторі. Внаслідок цього збільшується залежність державного й приватного секторів від стійкості й безпеки цифрових сервісів, що об’єктивним чином робить актуальним питання ідентифікації й розгляду головних кіберзагроз, котрі перед ними виникають на нинішній фазі розвитку.

Як відомо, «у 2024 році кількість кібератак на Україну зросла майже на 70%, досягнувши 4315 інцидентів, у порівнянні з 2541 роком раніше. Найчастіше хакери атакують критично важливу інфраструктуру: енергетичний сектор, урядові установи, органи безпеки та телекомунікації. Їх метою є викрадення чутливої інформації та знищення даних. Найпоширенішими інструментами є масові розсилки шкідливого програмного забезпечення та фішингові листи. Під час війни найціннішою для ворога є інформація про плани сил оборони України, дані підприємств оборонно-промислового комплексу, уряду та інших організацій, які здійснюють підтримку військових» [70]. При цьому, «від початку 2025 року Національна команда реагування на кіберінциденти, кібератаки, кіберзагрози CERT-UA фіксує в середньому близько 15 кіберінцидентів на день та відстежує понад 150 кластерів кіберзагроз (UAC). В основному кібератаки здійснюють пов'язані з Росією хакери [52]. Йдеться про:

– «UAC-0010 або Gamaredon/Primitive Bear/Aqua Blizzard (одна з найбільших загроз в контексті кібератак);

– UAC-0184, UAC-0200 (спеціалізуються на атаках на військовослужбовців);

– UAC-0218 / UAC-0219 (викрадення даних);

– UAC-0050, UAC-0006 (є найактивнішими фінансово вмотивованими кластерами)» [52].

Техніки, прийоми й операції хакерів весь час зазнають змін, ставлячи вимогу щодо постійного моніторингу, вивчення їх активності й обміну даними на глобальному рівні. Загалом, на сьогоднішній день основні кіберзагрози включають:

1. «Збільшення атак на критичну інфраструктуру. Зростання кібератак на державні установи, енергетичні системи, транспортні мережі та фінансові установи. Головною метою таких атак є дестабілізація країни, порушення роботи важливих сервісів та викрадення даних.

2. Фішинг та соціальна інженерія. Зловмисники все частіше використовують методи соціальної інженерії, зокрема підроблені електронні листи та повідомлення, які змушують користувачів передавати конфіденційну інформацію або встановлювати шкідливе програмне забезпечення.

3. Розвиток діпфейків та маніпуляція інформацією. Штучний інтелект значно вдосконалив технології діпфейків, що дозволяє створювати фальшиві відео та аудіозаписи для маніпуляції суспільною думкою або здійснення шахрайських дій.

4. Використання легітимних інструментів для атак (Living Off the Land). Хакери все частіше використовують легальні програми та адміністративні інструменти для проведення атак, що ускладнює їх виявлення традиційними засобами захисту» [67].

Зазначимо, що один з найбільш розповсюджених типів кіберзлочинів – застосування шкідливого програмного забезпечення. Це програма чи код зроблені для того, щоб завдати шкоди комп’ютеру, мережі або серверу. Згадане поняття охоплює велику кількість підмножин:

1. «Програми-вимагачі. Використовуючи їх, зловмисник шифрує дані жертви та пропонує ключ-розшифровки в обмін на гроші. Зазвичай такі атаки здійснюються через шкідливі посилання, які приходять на електронну пошту у вигляді фішингових листів.

2. Безфайлове шкідливе ПЗ. Це унікальна форма шкідливої активності, яка не вимагає встановлення коду на цільову систему, що ускладнює його виявлення. Замість цього воно використовує легальні інструменти, вже наявні в системі, для здійснення кібератак.

3. Шпигунське програмне забезпечення. Тип небажаного шкідливого програмного забезпечення, яке таємно заражає комп’ютер або пристрій і збирає інформацію про користувача без його відома або згоди. Воно спеціально розроблене для моніторингу дій користувача в Інтернеті.

4. Рекламне ПЗ. Особливий тип шпигунських програм, відстежує активність користувача в Інтернеті, щоб визначити, яку рекламу йому

показувати. Хоча рекламне ПЗ не обов’язково шкідливе, воно може негативно впливати на продуктивність пристрою і погіршувати користувацький досвід.

5. Троян. Трояни маскуються під легальне програмне забезпечення, щоб обманом змусити користувачів завантажити їх. Вони можуть бути встановлені через фішингові або підроблені сайти. Наприклад, варіант трояна Zeus спеціально націлений на фінансову інформацію і має на меті додати комп’ютери до бот-мережі.

6. Хробаки. Є окремими програмами, які розмножуються і поширюють свої копії на інші комп’ютери. Вони заражають свої цілі через вразливості програмного забезпечення або фішингові атаки. Хробаки можуть виконувати різні шкідливі дії, такі як модифікація файлів, впровадження нових шкідливих програм або реплікація до тих пір, поки цільова система не буде перевантажена.

7. Руткіти. Це тип шкідливих програм, які дають зловмисникам контроль над комп’ютерною мережею або додатком. Після активації руткіти встановлюють експлойт, який потім може бути використаний для розповсюдження інших шкідливих програм» [101].

DoS та DDoS атаки. Це дія, націлена на те, щоб заповнити мережу помилковими запитами, котрі порушують функціонування сервісу. В ході атаки в користувачів не має змоги здійснювати звичні завдання. Приміром, вони не можуть одержати доступ до електронної пошти, вебсайтів, облікових записів та ін. Переважне число подібних процесів не спричиняють втрати інформації та їхню дію можливо порівняно легко усунути, проте компанії витрачають багато часу й фінансів, щоб відновити роботу.

Ще одним найпоширенішим видом кіберзлочину є фішинг. Це метод кібератаки, що включає застосування різноманітних каналів, як-от електронна пошта, SMS, телефон, соціальні мережі, аби через обман примусити жертву поділитися конфіденційними даними чи завантажити шкідливе програмне забезпечення. Фішингові атаки, як правило, виконуються шляхом надсилання шкідливих електронних листів, котрі одержують певні люди чи організації.

Спуфінг – це техніка, котру застосовують для того, аби видати себе за надійне джерело задля одержання несанкціонованого доступу до систем та приладів. Це можуть здійснювати через різні методи, як-от підробка домену, підробка електронної пошти й підробка ARP. Під час підміни доменів зловмисники розробляють фальшиві вебсайти чи поштові домени, котрі є надзвичайно схожими на справжні, аби спонукати користувачів їм довіряти. З першого погляду згадані підроблені домени можуть здаватися справжніми, проте під час ретельного дослідження проявляються незначні розрізнення. Спуфінг електронної пошти включає надсилання електронних листів із підробленими адресами відправників, котрі вдають із себе відомі компанії чи приватних осіб. Через те, що отримувач довіряє відправнику, він більш імовірно відкриє лист, що посилює ризик взаємодії зі шкідливими посиланнями чи вкладеннями.

Атаки на основі ідентифікації. Один з типів кіберзлочинів, котрі вкрай складно встановити. Зловмисник виконує злом облікового запису користувача та маскується під нього. Нерідко вкрай складно знайти хакера, застосовуючи усталені заходи безпеки й засоби. Найпоширенішими атаками на основі ідентифікації є:

1. «Kerberoasting. Зловмисник намагається зламати пароль облікового запису служби в середовищі Active Directory.

2. Атака «людина посередині». Тип кібератаки, під час якого зловмисник підслуховує розмову між двома особами з метою збору особистих даних, паролів, банківських реквізитів тощо.

3. Атака Pass-the-Hash. Передача хешу (PtH) – це тип атаки, під час якої зловмисник викрадає «хешовані» облікові дані користувача та використовує їх для створення нового сеансу користувача в тій самій мережі.

4. Golden Ticket. Зловмисник намагається отримати необмежений доступ до домену організації, використовуючи вразливості в протоколі автентифікації. Отримуючи доступ до даних користувачів, що зберігаються в Microsoft Active Directory, хакер обходить методи автентифікації.

5. Silver Ticket. Зловмисник створює фальшивий квиток автентифікації, відомий як «срібний квиток», після викрадення пароля облікового запису. Цей квиток зашифрований і дозволяє доступ до ресурсів певного сервісу, на який спрямована атака.

6. Збір облікових даних. Це практика масового збору облікових даних користувачів, таких як ідентифікатори, адреси електронної пошти, паролі та інша інформація для входу. Це дозволяє кіберзлочинцям отримувати доступ до систем, збирати конфіденційні дані або продавати їх.

7. Заповнення облікових даних. Люди схильні повторно використовувати одні й ті ж облікові дані для входу в декілька облікових записів. Це означає, що якщо зловмисник отримує доступ до одного набору облікових даних, він потенційно може використати їх для доступу до інших облікових записів» [101].

Атака з інтеграцією коду. Зловмисник вводить шкідливий код у вразливий комп'ютер чи мережу з метою зміни їх роботи. Є різні види атак на введення коду:

1. «SQL-ін'єкція використовує вразливості в додатках, що керують даними, шляхом введення шкідливих SQL-запитів, що дозволяє зловмиснику витягувати інформацію з бази даних.

2. Міжсайтовий скриптинг (XSS) передбачає вставку шкідливого коду на легітимний веб-сайт, який запускається як інфікований скрипт у браузері користувача.

3. Зловмисна реклама виникає, коли зловмисник зламує сторонній сервер, вставляє шкідливий код в медійну рекламу і заражає комп'ютер користувача, коли той натискає на оголошення.

4. Отруєння даних – це кібератака, коли зловмисник маніпулює навчальним набором даних для моделі штучного інтелекту або машинного навчання, вносячи упередження, помилкові результати, впливаючи на її прогностичні можливості тощо» [101].

Психологічний тиск. Часом кіберзлочинці здійснюють атаки, що мають зв’язок із психологічним тиском, знані також як атаки соціальної інженерії. Хакери, застосовуючи такі сильні стимули, як любов, фінанси, тривога, статус, спонукають осіб надавати конфіденційні дані. Атаки соціальної інженерії класифікуються на кілька типів:

1. «Претекстування. Кіберзлочинці видають себе за іншу особу, когось, кому можна довіряти. Наприклад, за інвестиційного банкіра, працівника відділу кадрів або IT-спеціаліста, щоб обдурити жертву.

2. Компрометація ділової електронної пошти (BEC) полягає в тому, що зловмисник видає себе за довіреного користувача, щоб обманом змусити співробітників або клієнтів поділитися конфіденційними даними або здійснити платежі.

3. Дезінформаційні кампанії – ще одна форма соціальної інженерії, яка спрямована на поширення неправдивої інформації з політичних або воєнних мотивів. Зловмисники використовують соціальні мережі, ботів і фейкові акаунти, щоб посилити свої неправдиві наративи і створити відчуття консенсусу.

4. Quid Pro Quo. Зловмисники пропонують користувачеві оплатити товар чи послугу, не завжди надаючи їх.

5. Honeytrap. Атаки типу «медова пастка» відбуваються на додатки/сайти знайомств, де зловмисники створюють фальшиві профілі, щоб обманом змусити жертв поділитися грошима, інформацією або доступом до мережі» [101].

Атаки з використанням штучного інтелекту. Зі зростанням технологій штучного інтелекту й машинного навчання зловмисники, крім того, стали застосовувати зазначені інструменти в своїх інтересах. Зокрема постав темний ШІ – вид штучного інтелекту, що визначає і використовує вразливості чужих мережевих систем. Крім того, зловмисниками застосовуються діпфейки, фейкові чат-боти й віртуальні помічники, аби виманити в користувачів конфіденційні дані, здійснити вплив на думку громадськості, залякати та ін.

Варто зауважити, що синхронізовані процеси здійснюються, коли кібератаки сполучаються з дезінформацією і синхронізуються із військовими діями. Приміром, кібератаки на енергетичну інфраструктуру України супроводжувалися масованими обстрілами. До взаємодоповнюючих процесів можливо зарахувати розповсюдження дезінформації в результаті кібератак. У табл. 2.1 проведемо SWOT-аналіз ефективності реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України. Ефективність реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України доречно досліджувати в розрізі сильних сторін, що утворилися останніми роками. Передусім мова йде про існування базового нормативно-правового і стратегічного підґрунтя, що формує цілі, принципи та суб'єктів державної політики в секторі кібербезпеки. Крім того, вагома перевага – інституційна фіксація відповідальності за координацію і реагування на кіберзагрози, і, до того ж, нагромаджений практичний досвід протидії масштабним кібератакам на тлі гібридної і повномасштабної війни. Додатковий фактор зростання результативності – активне міжнародне співробітництво і сприяння зі сторони стратегічних партнерів, що допомагає посилити кіберстійкість державної сфери.

Водночас реалізація механізмів публічного управління у сфері кібербезпеки супроводжується низкою системних слабких сторін. З-поміж них основними продовжують залишатися фрагментарність повноважень між різними органами влади, недостатній ступінь міжвідомчої координації, а також нерівномірність введення заходів кіберзахисту на центральному й місцевому рівнях. Велика проблема – брак кваліфікованого персоналу й, крім того, обмежений фінансовий й матеріально-технічний потенціал, через що ускладнюється практична імплементація стратегічних документів та погіршується загальна ефективність державної політики в згаданій галузі.

Таблиця 2.1

SWOT-аналіз ефективності реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України.

Сильні сторони (Strengths)	**Слабкі сторони (Weaknesses)**
Сформована нормативно-правова база у сфері кібербезпеки (стратегія, закони, підзаконні акти).	Наявність фрагментарності повноважень та недостатньої координації між суб'єктами, що виконують функції у сфері забзепечення кібербезпеки.
Наявність інституційної визначеності ключових суб'єктів (РНБО, СБУ, Держспецзв'язку та ін.).	Недостатність фінансових та матеріально-технічних ресурсів, особливо на локальному рівні.
Набуття практичного досвіду протидії масштабним кібератакам, що поширюються у ході повномасштабного вторгнення рф на територію України.	Обмеженість кваліфікованих кадрів у сфері кібербезпеки, на які покладено функції забезпечення кібербезпеки.
Формування активної міжнародної підтримки та співпраці з партнерами (США, ЄС, НАТО).	Нерівномірність забезпечення кіберзахисту в органах державної влади та об'єктах критичної інфраструктури.
Розвиток інтеграції кібербезпеки в практичну діяльність інституцій, що відповідають за забезпечення національної безпеки та оборони.	Повільний темп імплементації окремих стратегічних і програмних документів у практичній діяльності.
Можливості (Opportunities)	**Загрози (Threats)**
Подальший розвиток нормативно-правового забезпечення у сфері кібербезпеки України відповідно до європейських та євроатлантичних стандартів.	Поширення постійних та високотехнологічних кібератак з боку рф.
Формування державно-приватного партнерства у сфері кіберзахисту.	Зростаюча складність кібератаки, що ґрунтуються на використанні штучного інтелекту та автоматизованих засобів.
Зміцнення міжнародних відносин у сфері фінансової та технічної допомоги задля того, щоб модернізувати систему кіберзахисту.	Поява високої залежності від іноземних технологій та програмного забезпечення для цілей забезпечення кібербезпеки.
Удосконалення цифрової освіти та підготовки фахівців у сфері кібербезпеки серед працівників органів публічного управління.	Наявність ризиків витоку чутливої інформації та компрометації інформації, що розміщена на державних інформаційних ресурсах.
Розробка та реалізація єдиної національної системи моніторингу та реагування на поширення кіберінцидентів.	Недостатня кіберкультура та обізнаність користувачів державних послуг.

Джерело: власна розробка автора

Разом із тим сучасні умови відкривають значні можливості для підвищення ефективності механізмів публічного управління кібербезпекою. Насамперед це має відношення до узгодження національного законодавства зі

стандартами ЄС і НАТО, зростання державно-приватного партнерства і, крім того, залучення міжнародної фінансової і технічної підтримки для того, щоб модернізувати інформаційно-комунікаційні системи. Перспективний вектор, крім того, – зростання системної підготовки і підвищення кваліфікації персоналу в секторі кібербезпеки, що дасть можливість посилити інституційну спроможність органів публічної влади.

Водночас реалізація потенційних можливостей відбувається в умовах значних загроз, що негативно впливають на ефективність публічного управління у сфері кібербезпеки. Безперервні кібератаки зі сторони країни-агресора, посилення складності кіберзагроз із застосуванням новітніх технологій і, крім того, ризики витоку чутливих даних формують додаткове навантаження на систему публічного управління. В комплексі з недостатнім ступенем кіберкультури певних груп працівників і залежністю від іноземних технологій згадані загрози ставлять вимогу щодо наступного покращення механізмів публічного управління і поглиблення комплексного підходу до гарантування кібербезпеки України. В Україні вже вводяться комплексні заходи, щоб протидіяти кіберзагрозам. З-поміж головних ініціатив:

1. Зростання Державного центру кіберзахисту при РНБО, котрий несе відповідальність за моніторинг загроз та оперативне реагування на атаки.

2. Зміцнення законодавчої основи в секторі кібербезпеки, включно з обов’язковою сертифікацією критичної інфраструктури.

3. Співробітництво із міжнародними партнерами, як-от НАТО, Європейський Союз і США, для того, щоб обмінюватися досвідом і вводити нові технології захисту.

4. Навчання і підготовка фахівців у сфері кібербезпеки, що передбачає сприяння навчальним програмам у вишах і спеціалізовані курси.

За прогнозом, наступні технології будуть гарантувати максимальний розвиток ринку впродовж наступного п’ятиріччя (див. табл. 2.2).

Таблиця 2.2

Найбільший ріст ринку кіберзахисту протягом наступних 5 років

Сегмент	Ріст до 2029 р.	Характеристика
Безпека хмарних сервісів	+3,78млн дол. або 226%	• Сегмент, що охоплює захист середовищ та даних, розміщених у хмарі. • Прогнозується ріст поширення хмарних сервісів, при цьому зберігатиметься переважання традиційних методів зберігання даних у деяких секторах бізнесу. • Прогнозований лідер росту у відсотковому вимірі.
Безпека кінцевих точок	+6,08млн дол. або 85,8%	• Сегмент розуміє під собою захист пристроїв, які підключені до корпоративної мережі. • Паралельно зі зростанням поширеності віддаленої роботи, очікується сталий ріст цього сегменту (другий показник, як у відсотковому, так і у грошовому вимірах).
Безпека мережі	+29,4 млн дол. або 63,5%	• Сегмент означається сукупністю заходів та потужностей, спрямованих на недопущення несанкціонованого проникнення в мережу. • Очікується послідовне зростання, котре становитиме найбільшу в кількісному вимірі частку ринку.
Інше	+14,03 млн дол. або 58,1%	• Серед іншого, включає безпеку додатків, даних тощо. • Прогнозується пропорційне помірне зростання, котре відбуватиметься паралельно зі зростанням використання просунутих інформаційних технологій у різних галузях бізнесу.

Джерело: розроблено за матеріалами [106]

Прогноз розвитку ринку кіберзахисту вказує на структурні зміни й диференціацію динаміки збільшення між певними частинами. Найбільші темпи приросту у відсотковому контексті передбачаються в секторі безпеки хмарних сервісів, котрий до 2029 р. збільшиться на 226 % (+3,78 млн. дол. США). Це спричинено послідовною міграцією бізнесу і державних органів до хмарних середовищ, потребою захисту розподілених даних та сервісів і, крім того, зростанням вимог щодо безпеки під час застосування SaaS-, PaaS- та IaaS-рішень. Незважаючи на те, що в деяких секторах буде зберігатися переважання усталених моделей зберігання інформації, якраз згаданий

сегмент буде виступати лідером збільшення відповідно до відносних показників.

Другим за динамікою росту буде сегмент безпеки кінцевих точок, що покаже приріст на 85,8 % чи 6,08 млн. дол. США. Такий розвиток прямо пов’язаний зі збільшенням числа приладів, які підключені до корпоративних мереж і, крім того, розповсюдженням віддаленої й гібридної форм зайнятості. В зазначених обставинах захист робочих станцій, мобільних пристроїв та IoT-рішень являється критично значущою складовою кібербезпеки як для бізнесу, так і для публічної сфери.

В той же час сегмент безпеки мережі, хоч і поступається за відсотковою динамікою зростання (63,5 %), гарантуватиме максимальний абсолютний приріст – 29,4 млн. дол. США. Це вказує на його переважаюче значення в структурі ринку кіберзахисту. Систематичне збільшення зазначеного сегмента спричинене потребою комплексного захисту мережевої інфраструктури від несанкціонованого доступу, кібератак та порушень цілісності інформації, насамперед на тлі воєнних і гібридних загроз.

Сегмент «інше», який включає безпеку додатків, інформації, а також суміжні вектори, збільшиться на 58,1 % чи 14,03 млн. дол. США, показуючи помірну, проте стабільну динаміку. Його зростання здійснюватиметься одночасно із введенням провідних інформаційних технологій в різного роду сферах економіки й публічного управління. В цілому прогнозована структура зростання ринку кіберзахисту вказує на послідовний перехід від усталених моделей безпеки до більш комплексних та адаптивних рішень, які є відповідними нинішнім викликам цифрової сфери.

Підсумовуючи, зауважимо, що попри те, що є п’ятдесят п’ять державних університетів, де пропонуються освітні програми із кібербезпеки, а мінімум шістнадцять приватних IT-шкіл здійснюють надання спеціалізованих програм, розрив якості між державною і приватною освітою вважається істотним. Співвідношення державних та приватних програм 3.5:1 акцентує на тому, що кількість не дорівнює якості, оскільки:

1. Неіснування практичних навичок: велика кількість університетів не забезпечують студентам потрібних практичних навиків щодо кібербезпеки, що спричиняє брак практичного досвіду й спеціальних знань, які необхідні в секторі кібербезпеки.

a. Перехід до загальних IT-ролей: з огляду на недостатню підготовку велика кількість студентів у підсумку працює на загальних IT-ролях, як-от фронт-ендабобек-енд розробка.

b. Приватним компаніям вдається заповнювати прогалини: пропонують великий перелік практичних програм і спеціалізованих курсів, практичну підготовку з кібербезпеки, враховуючи вимоги професійних стандартів і вимоги індустрії.

Міжнародні програми допомоги, що вважаються головним джерелом фінансування використання продуктів і послуг у секторі кібербезпеки, у великому числі ситуацій обирають компанії зі свого вітчизняного ринку, не беручи до уваги існування пропозицій на ринку України.

Пролонгація подібної політики в значних обсягах – чинник для потенційної деградації ринку України.

Державі доречно ухвалити програми і вводити заходи, які повинні гарантувати зростання конкурентоспроможності вітчизняної індустрії із потенційною локалізацією R&D діяльності у секторі кібербезпеки, що реалізується у тому числі шляхом одержання унікальних даних на тлі кіберагресії проти України;

Державі доречно не лише на декларативному рівні визнати, а вводити принцип зростання державно-приватного партнерства як одного з пріоритетів державної політики у секторі кібербезпеки;

Індустрії доречно об’єднати власні зусилля за допомогою конференцій, комітетів, клубів для послідовного просування інтересів і взаємодії всіх стейкхолдерів кібербезпеки в Україні.

2.3. Проблеми реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України

В нинішніх обставинах динамічної цифровізації суспільства й збільшення залежності державних інституцій, бізнесу та громадян від інформаційно-комунікаційних технологій питання забезпечення кібербезпеки отримує статус одного з головних пріоритетів публічного управління. Кіберпростір трансформувався у повноцінний сектор суспільних відносин, в рамках котрого постають нові загрози національній безпеці, стабільності діяльності критичної інфраструктури, захисту персональної інформації, а також інформаційного суверенітету держави. По-особливому актуальними зазначені виклики стають в обставинах гібридних загроз, кібератак державного й недержавного походження і, крім того, застосування цифрових технологій як засобу політичного, економічного та воєнного впливу.

В еру цифрового врядування зростаюча залежність від інформаційних систем спричинила зміни парадигми публічного управління. Згадане перетворення, забезпечуючи безпрецедентну результативність та доступність, в той же час наразило державу на безперервно зростаючу загрозу кіберінцидентів. Кібербезпека виявилася базисом щодо гарантування безперебійної діяльності й цілісності фнкціонування держави. Ю. Чаплінська зауважує, що «прогрес у цифровізації публічного управління та бізнесу відкриває нові можливості, проте формує й нові загрози, зокрема кіберзлочинність, яка стає дедалі витонченішою. Цифровізація змінює характер злочинності, створюючи вразливості через інтеграцію технологій у повсякденне життя» [163]. О. Червяков також вважає, що «необхідно бути свідомими щодо того, що в останні десятиліття проблема кібербезпеки суттєво трансформувалася з рівня окремого комп’ютера на рівень держави, окремих організацій, сфер економіки та об’єктів критичної інфраструктури. З огляду на це, дана проблема тепер не є суто технічною, а має розглядатися саме з точки

зору адміністративно-правового забезпечення функціонування цілісного механізму забезпечення кібербезпеки держави, створення відповідних інституцій, центральних органів виконавчої влади, відповідальних за даний напрямок, а також структурних підрозділів (посадових осіб) на рівні окремих підприємств, установ, організацій» [164].

Зауважимо, що «усе, що використовує технології, базується на комунікаційних та інформаційних системах, а це означає, що це залежить від кібербезпеки. Державний і приватний сектори щороку витрачають мільйони доларів на технології, програмне забезпечення безпеки та апаратні пристрої, які підвищують кібербезпеку в компаніях, але вони все ще вразливі. Основна проблема цієї ситуації полягає в тому, що кібербезпека все ще зазвичай розглядається як технічний аспект або технологія, яку можна легко впровадити всередині організації, і ця реалізація гарантуватиме кібербезпеку. Це ставлення має змінитися, тому що кібербезпека сьогодні – це щось більше, ніж просто технології» [192]. Варто погодитись з О. Костенко, що «на міжнародному і національному рівнях кіберзлочинність є однією з найгостріших проблем, яка постала сьогодні перед публічними органами усіх держав. Досі не вироблений системний підхід у протидії кіберзлочинності з урахуванням сучасних викликів і загроз інформаційній безпеці» [80].

Як зауважує А. Вовк, «транскордонний характер кіберпростору, який спільно використовується безліччю агентів інформаційних та комунікаційних систем, створюють труднощі у вирішенні завдання попередження загроз кібербезпеці. Стратегії, що реалізуються державою, організаціями та окремими індивідами внаслідок їх тісного взаємозв’язку можуть мати суттєві наслідки для інших агентів усередині країни та за її межами, а також впливати на стан цифрового простору. В даний час комп’ютерні атаки неухильно зростають як за кількістю, так і за складністю. Вони стають дедалі цілеспрямованішими і зачіпають не лише державу, а й приватний сектор. У цих умовах держава починає усвідомити стратегічну важливість даних та

контролю над ними, а також необхідність створення надійної системи захисту від кіберризиків» [19].

Р. Лук'янчук зазначає, що «з огляду на рівень проникнення ІКТ у всі критично важливі сфери життєдіяльності людини та держави, не виключається бажання деяких держав світу продемонструвати своє домінування у міжнародному кіберпросторі. Крім того, це призводить до необхідності чіткої регламентації засад державної політики більшості провідних держав в питанні контролю за власним кіберпростором, передбачає необхідність визначення пріоритетів державного управління кібербезпекою. Активність з боку провідних держав світу у кіберпросторі, формування потужних транснаціональних злочинних хакерських груп, що спеціалізуються на злочинах в кіберпросторі, обумовлюють необхідність вдосконалення вітчизняного безпекового сектору» [91]. Американські дослідники S. Ganapati, M. Ahn, C. Reddick стверджують, що «існує дихотомія у трактуванні кібербезпеки як технічної проблеми чи проблеми управління. Вчені з публічного управління вважали кібербезпеку, імовірно, технічною проблемою, хоча політика безпеки діє з середини 1980-х років. Технічні проблеми еволюціонували від проблем окремих комп'ютерів (наприклад, віруси) до проблем системної мережі (наприклад, атаки програм-вимагачів). Останні публікації демонструють розгляд кібербезпеки саме як проблеми управління» [184].

На сьогоднішній день, «Україна перебуває на етапі активної цифрової трансформації, яка охоплює державний і приватний сектори. Впровадження електронного урядування, зокрема платформи «Дія», спрощує доступ до послуг і підвищує прозорість управління. У бізнесі цифровізація проявляється зростанням електронної комерції, автоматизацією процесів та використанням хмарних технологій, CRM-систем і IT-інфраструктур для аналізу даних та управління» [42]. Однак, «попри активний розвиток цифрових технологій, Україна стикається з низкою проблем. Серед них – нерівномірність доступу до цифрових інструментів між різними регіонами, недостатній рівень цифрової

грамотності значної частини населення та низька захищеність багатьох інформаційних систем від кіберзагроз» [11]. Це формує вагомі виклики для гарантування результативності цифровізації, а також її безпечності як в державній сфері, так і в секторі бізнесу. Важливо розуміти, що «сучасна Україна також стикається з тяжкими проблемами в забезпеченні захисту своєї економічної системи та її суб'єктів під час повномасштабного вторгнення російської федерації. Як молода держава, Україна має нестачу стресостійкості у своїй економічній системі, порівняно з країнами-союзниками» [159].

В еру конфліктів економічна система України має ключове значення щодо підтримки бойової готовності її армії. Наші вороги усвідомлюють це й стараються її дестабілізувати. Останніми роками прослідковується істотне розповсюдження схем махінацій, що основуються на банківській системі і базуються на фішингу. Так, «фішингові атаки через фейкові сайти та електронні листи, що виглядають як листи від реальних банків, чинять шкоду не лише окремим особам, але й довірі до держави в цілому. Втрата довіри призводить до репутаційних проблем, що ускладнює повноцінну діяльність та має негативний вплив на державу загалом» [159].

С. Бабанін також додає, що «цифровізація в Україні модернізує публічне управління та бізнес, підвищуючи ефективність і створюючи нові можливості. Однак швидке впровадження технологій випереджає розвиток систем захисту, що робить установи й бізнес вразливими до кіберзлочинців, що вимагає аналізу типів таких злочинів, їхньої специфіки та впливу на ключові сфери діяльності» [9]. З-поміж найбільш розповсюджених видів таких злочинів можливо виділити:

1. «Кібератаки на державні системи та бізнес-інфраструктуру загрожують цифровому середовищу, спричиняючи економічні збитки, дискредитацію управління та порушення роботи організацій. Атаки типу DDoS і віруси, як-от Petya/NotPetya, завдають значної шкоди державним і приватним установам.

2. З розвитком електронного урядування зростають випадки несанкціонованого доступу до персональних даних через фішинг, шкідливі програми чи злами баз. Це загрожує фінансовими втратами, крадіжкою особистості та маніпуляцією інформацією.

3. Фінансові шахрайства в електронному середовищі включають злами банківських систем, підробку транзакцій, фішинг та шахрайства з криптовалютами. Ці загрози супроводжують цифровізацію й потребують ефективних заходів для захисту держави, бізнесу та громадян.

4. Однією з основних вразливостей державного сектору є недосконаліть захисту даних, яка полягає у використанні застарілих систем, недостатньому оновленні програмного забезпечення та слабкій інтеграції сучасних технологій безпеки. Наприклад, багато державних органів все ще використовують програми, які не мають належного рівня захисту, що робить їх вразливими до атак зловмисників. Зокрема, нерідко відсутні комплексні системи моніторингу кіберзагроз, які могли б виявляти атаки на ранніх стадіях.

5. Низька обізнаність працівників державних установ щодо кіберзагроз і відсутність чітких стратегій реагування на атаки підвищують ризик несанкціонованого доступу до даних, порушення роботи органів та зниження довіри громадян. Подолання цих проблем вимагає впровадження технічних рішень, підвищення цифрової грамотності та розробки ефективних стратегій кіберзахисту» [42].

Як зазначає К. Герасимюк, «сьогодні в Україні накопичилася ціла низка кібер- та інформаційних загроз і викликів. Адже значною загрозою безпеці держави є і тотальне використання невітчизняного програмного забезпечення та сервісного зберігання інформації щодо всіх сфер діяльності органів публічної влади. До цього часу немає на 100 % нормативно урегульованих конкретних стандартів і вимог до інформаційних систем державних органів влади та місцевого самоврядування. А це означає, що сьогодні значна частина цих органів послуговуються програмним продуктом досить сумнівного

походження (в тому числі і з країни-агресора, і з приватних міжнародних структур). Наприклад, з настанням пандемії всі структури публічного та приватного секторів, звичайні громадяни вимушені були для дистанційної роботи / навчання використовувати платформу Zoom, яка при завантаженні апріорі має доступ до налаштувань гаджета користувача, а отже і до всієї інформації на ньому з можливістю її подальшого відстеження» [23]. Таким чином, наразі доволі умовно можливо стверджувати про відповідальність державного службовця й посадовця місцевого самоврядування, і, врешті-решт, навіть лікаря, щодо додержання службової таємниці. Також на рівні законодавства зазначені питання теж не врегульовано до кінця. Зростання числа кіберзлочинів – комплексна проблема, якій притаманні як загальні, так і спеціальні причини, а саме:

1) «висока завантаженість правоохоронних органів. Причинами цього є обмеженість ресурсів правоохоронних органів, які змушені розглядати широкий спектр правопорушень та нестача спеціалістів, здатних розслідувати кіберзлочини.

2) анонімність та глобальний характер кіберзлочинів. Така ситуація пов’язана з можливістю приховування особи через VPN, Tor та інші засоби анонімізації, а також географічною розподіленістю злочинців, яка ускладнює юрисдикційні питання.

3) стрімкий технологічний прогрес. Так, постійно впроваджуються нові технології, які кіберзлочинці активно експлуатують.

4) брак кібергігієни. Причиною цього є недостатня обізнаність користувачів про безпечну поведінку в Інтернеті та відсутність відповідальності за недотримання кібергігієни» [150].

Як зазначає В. Лазарів, «однією з найбільш поширених кіберзагроз є атаки типу ransomware, коли зловмисники блокують доступ до інформації або систем і вимагають викуп за їх відновлення. Це може призвести до серйозних перебоїв у роботі органів публічного управління, зокрема в ситуаціях, що потребують оперативного реагування, наприклад, під час надзвичайних

ситуацій. Іншим поширеним типом є фішинг-атаки, що спрямовані на отримання доступу до конфіденційної інформації шляхом обману працівників державних установ Через низький рівень цифрової грамотності або недостатню увагу до кібербезпеки такі атаки часто виявляються успішними. Особливу небезпеку становлять Distributed Denial of Service (DDoS) атаки, які блокують роботу електронних послуг, перевантажуючи сервери надмірною кількістю запитів. Такі атаки не лише призводять до тимчасового припинення роботи державних сервісів, але й підривають довіру громадян до електронного урядування. Наприклад, в Україні DDoS-атаки неодноразово використовувалися для дестабілізації роботи критичної інфраструктури під час гібридної війни» [87].

Ще однією актуальною загрозою є «використання вразливостей у програмному забезпеченні. Зловмисники активно шукають недоліки в системах електронного урядування, які можуть дозволити їм отримати доступ до внутрішніх ресурсів або викрасти конфіденційні дані. В умовах глобалізації та збільшення кількості постачальників IT-рішень для публічного сектору це питання набуває особливої актуальності, адже державні установи не завжди мають ресурси для регулярного оновлення програмного забезпечення чи тестування на наявність вразливостей. Також викликають занепокоєння загрози, пов’язані з використанням новітніх технологій, таких як штучний інтелект та Інтернет речей (IoT). Наприклад, компрометація пристроїв IoT, які використовуються у смарт-містах, може призвести до масштабних збоїв у роботі критичної інфраструктури, такої як системи управління транспортом або енергопостачанням. А використання штучного інтелекту для автоматизації атак дозволяє хакерам діяти швидше та ефективніше» [87].

Круглов зазначає, що «забезпечення надійних заходів кібербезпеки державних інформаційних ресурсів є надзвичайно важливим, оскільки в цих системах зберігаються конфіденційні дані та об’єкти критичної інфраструктури, необхідні для функціонування державних органів та національної безпеки» [84]. Незважаючи на існування в Україні нормативно-

правової основи, а також інституційної архітектури в секторі кібербезпеки, практика втілення механізмів публічного управління встановлює ряд системних проблем, що спричиняє необхідність щодо переосмислення наявних підходів до створення і втілення державної політики у сфері кібербезпеки. З огляду на це дослідження проблем реалізації механізмів публічного управління у сфері забезпечення кібербезпеки – вагоме в науковому й практичному аспектах.

Масовий перехід переважного числа галузей діяльності людей у віртуальний простір спричиняє потребу напрацювання нових систем гарантування кібер- та інформаційної безпеки. В нинішніх умовах, які відзначаються гібридними війнами, глобальною пандемією, міжнародними й регіональними економічними потрясіннями, зазначене питання стає по-особливому актуальним. Воно має зв’язок із утворенням великої кількості загроз для держав, бізнесу, соціуму загалом і певних людей зокрема. Для органів публічного управління згадана проблема відіграє критичну роль, тому що має відношення до ризиків, які мають зв’язок з обігом та захистом даних. Тотальна цифровізація даних, їх зберігання, передавання і застосування формують істотні виклики, з-поміж котрих неналежне застосування, пошкодження або перетворення даних і, крім того, зовнішні несанкціоновані втручання. Подібні загрози здатні зашкодити як державі, так і певним особам.

В сьогоденні електронні послуги виявилися невід'ємною складовою діяльності публічних органів. У той же час їх застосування супроводжується постанням різних кіберзагроз, що небезпечно для результативності, постійності й безпеки надання зазначених послуг. Важливим зауваження є те, що поширене розповсюдження цифрових технологій в усі сектори життєдіяльності суспільства на сучасному етапі обумовлює те, що ІТ-компанії стають повноправними учасниками системи кібербезпеки держави. Це спричинено тим, що сформовані ними інформаційні системи вважаються об’єктом кібератак. Й це спонукає їх здійснювати розробку устаткування і програмного забезпечення, які застосовуються для того, щоб виявляти і

захищатися від кіберінцидентів. Зважаючи на це, співробітництво між державною сферою і ІТ-компаніями – необхідна передумова гарантування кібербезпеки держави.

Оскільки «інформаційні системи стають невід'ємною частиною процесу прийняття рішень, надання послуг та комунікації в органах публічної влади, вразливість систем до кіберзагроз становить значний ризик. Кібербезпека стала критично важливим компонентом, що формує стійкість і надійність публічного управління» [77]. Зауважимо, що «швидка еволюція кіберзагроз, таких як сучасні постійні загрози, атаки з вимогою викупу та складне шкідливе програмне забезпечення, становить значний ризик для державних мереж та систем. Суб'єкти загроз, включаючи інші держави та кіберзлочинні організації, постійно розробляють нові технології та використовують вразливості, що ускладнює роботу органів влади, які не встигають за постійними змінами» [66].

Варто також зауважити, що «небезпека кібербезпеки посилюється характеристиками мереж 5G. Споживачі, підприємства та міста по всій країні, які намагаються впровадити 5G, погано підготовлені для оцінки та усунення пов'язаних з ним небезпек. Як рішення вкрай важливо визначити особи сторонніх зловмисників, залучених у безперервний процес отримання незаконного доступу до даних користувачів та зловживання їхньою конфіденційністю та довірою до фірм або держави» [19.]. Відтак, «зловмисники можуть запускати атаки на системи на основі блокчейну. Багато з цих атак використовували добре відомі методи, такі як фішинг, соціальна інженерія, атаки на дані при передачі та зосередження уваги на помилках кодування. Можна створити більш надійну технічну інфраструктуру за допомогою засобів контролю та стандартів кібербезпеки на основі блокчейну для захисту підприємств від кібератак. Також може знадобитися поєднання блокчейна з іншими передовими технологіями, такими як штучний інтелект, Інтернет речей та машинне навчання» [19].

В той же час, «недоліки програмного забезпечення, які можуть надати зловмиснику доступ до системи, відомі як вразливості в програмному забезпеченні. Ці недоліки можуть бути результатом помилки у кодуванні програмного забезпечення або у тому, як воно побудовано. Програмне забезпечення, що управляє вразливістю, має стратегію кібербезпеки. Воно запобіжно сканує мережу на наявність вразливостей, виявляє їх та пропонує рекомендації щодо усунення недоліків, щоб знизити ймовірність порушень безпеки в майбутньому» [19].

При цьому, «додатковий виклик для забезпечення кібербезпеки створюють глобальні проблеми, зокрема зміни клімату, інновації у сфері міжнародної економіки та фінансів (наприклад, впровадження криптовалют, таких як біткоїн). Хоча ці явища на перший погляд не мають прямого зв’язку з електронним урядуванням, їхній вплив стає очевидним через залежність цифрової інфраструктури від надійного енергозабезпечення. Прості відключення електроенергії у громадах чи регіонах можуть призвести до тимчасового паралічу діяльності органів влади, а також до порушення прав громадян на доступ до інформації, підтвердження майнового стану чи ідентифікації особистості» [87].

За висловлюванням Б. Конюхова, «відсутність комплексної політики, стандартів і керівних принципів кібербезпеки в державних органах призвела до неузгодженості в практиках безпеки і недостатніх заходів захисту. Багато відомств покладаються на застарілі протоколи безпеки або не мають необхідних ресурсів і досвіду для ефективного впровадження надійних рішень з кібербезпеки» [77]. Крім того, «дедалі ширше використання хмарних обчислень, мобільних пристроїв та технологій Інтернету речей (IoT) в органах влади розширює сферу атак і створює нові вразливості. Забезпечення безпечної інтеграції та управління наявними технологіями залишається значним викликом, особливо в умовах бюджетного дефіциту та кадрових потреб» [77].

Як відомо, «в сучасних умовах кібератаки можуть бути здійснені з будь-якого місця, яке встановити та ідентифікувати є складним завданням: Інтернет-кафе, Wi-Fi системи або із застосуванням комп'ютерів третіх осіб. Вплив інформаційних загроз на структури державної влади, які відповідальні за підготовку і ухвалення рішень, реалізація яких безпосередньо впливає на безпеку країни, може призводити до виникнення надзвичайних ситуацій в державі і суспільстві, значним збиткам із-за порушення функціонування систем зв'язку, контролю і управління та просочування інформації, яка містить державну таємницю» [91]. Тому, «виходячи із реалій сьогодення, кіберпростір все ще залишається не повністю нормативно врегульованим на міжнародному рівні, тому спецоперації, що здійснюються в ньому військовими чи розвідувальними підрозділами, не підпадають під визначення «акту війни». Фактично, йдеться про можливість забезпечити ефект військового втручання без подальших офіційних санкцій як з боку держави, що зазнала нападу, так і світового співтовариства» [91].

Низку системних і управлінських проблем варто дослідити окремо, як такі, які не гарантують відповідний ступінь (індекс) кібербезпеки:

– «відсутність системності ведення кібердій, теорії застосування сил та засобів кібероборони, взаємодії різних відомств у сфері забезпечення кібероборони держави;

– відсутність в секторі оборони єдиного координуючого органу з питань забезпечення кібербезпеки та системи підготовки військового й цивільного персоналу;

– проблеми кадрового забезпечення відповідних структурних підрозділів та відтік за кордон кваліфікованих спеціалістів;

– зниження рівня наукового потенціалу, відсутність наукових шкіл, складнощі із методичним, науковим і технічним забезпеченням відтік за кордон кваліфікованих наукових кадрів» [16].

Розв'язати зазначені вище проблеми не можна без гармонізації, а також унормування термінологічних систем секторів кібербезпеки та кібероборони.

На тлі не розв’язання такого роду проблем вірогідні кіберзагрози здатні втілитися в успішні кібератаки на складні соціотехнічні системи держави, що спричинить постання критичних ситуацій (зокрема й техногенних аварій і катастроф. Так, ними можуть стати:

– «порушення управління державою та її інституціями шляхом здійснення деструктивних впливів на соціум (населення та політиків і керівників різного рівня з метою усунення та дискредитація осіб, які приймають рішення, формування негативної громадської думки про дії влади, спонукання населення до деструктивних дій тощо);

– використання глобальних інформаційних мереж терористичними та екстремістськими організаціями з метою організації терористичних актів, а також вербування нових бойовиків;

– несанкціоноване втручання в комп’ютерні мережі та системи управління органів державного та військового управління, стратегічно важливих об’єктів критичної інфраструктури, національних підприємств, управління військами та зброєю з метою отримання доступу до службової, конфіденційної або комерційної інформації, її викрадення, спотворення чи знищення, або/та взяття таких систем під контроль чи виведення їх з ладу» [16].

Кібербезпека в даному випадку відіграє вирішальну роль, тому що вона захищає від певних найбільш вагомих проблем в секторі кібербезпеки, як-от крадіжка і ліквідація великої кількості видів даних. Це містить конфіденційні дані, персональну інформацію, персональні дані, інформацію про інтелектуальну власність, а також інформаційні системи, як застосовує уряд і підприємства.

Зауважимо, що «інформаційне забезпечення протидії організованій злочинності в умовах збройного конфлікту не може бути організоване без забезпечення захисту інформації та кібербезпеки. Воєнний стан спричиняє суттєві зміни в підходах держави до захисту власного інформаційного та кіберпростору. Це, у свою чергу, впливає на ставлення до безпеки інформації,

засобів її оброблення та кіберсередовища, у якому вона передається, а також на визначення об’єктів впливу та реалізацію заходів із забезпечення інформаційної та кібербезпеки. Поточні обставини, у яких Україна розвиває власний інформаційний та кіберпростір, вимагають термінового впровадження глибоких і системних змін. Необхідність таких перетворень підтверджується кібератаками на об’єкти критичної інфраструктури та численними іншими інцидентами, які противники активно використовують проти нашої держави» [91]. Це здійснюється на фоні інтенсивного розвитку інформаційних технологій, збільшення технологічної складності зовнішніх загроз, активного застосування методології соціальної інженерії, ШІ, Інтернету речей, а також квантових технологій.

Як відомо, «з початком повномасштабної війни майже всі українські державні сайти, банківські сервіси, системи та інфраструктура зазнали величезної кількості ворожих кібератак та збоїв. Почалися атаки на офіційні сайти Верховної Ради України, Кабінету Міністрів України, Міністерства закордонних справ України, Служби безпеки України, Міністерства оборони України, Міністерства України з питань реінтеграції тимчасово окупованих територій, ПриватБанку та Ощадбанку, а також великої кількості інших установ» [167]. Загалом, «кібератаки були націлені на приховане викрадення важливої інформації, ймовірно, для надання Росії стратегічної переваги на полі бою. Все це відбувається для того, аби здійснювати психологічний тиск на громадян, дестабілізувати ситуацію всередині країни, посіяти паніку і хаос, паралізувати засоби комунікації й зв'язку у нашій державі. Посилюється тенденція здійснення розвідувально-підривної діяльності у кіберпросторі шляхом залучення різними спеціальними службами окремих держав, насамперед Росії, міжнародних хакерських угруповань для реалізації кібервпливу» [168].

Загроза кібератак зі сторони російської федерації як на системи України, так і на європейських партнерів продовжує залишатися значною. Нині кібербезпека – головне питання в економічному, політичному, соціальному й

військовому вимірах. Наразі Україна мусить захищати своє право на незалежність, на свій напрям розвитку і мирне та вільне майбутнє. Іншими словами, у вітчизняних правоохоронних органів з'являється дедалі більше завдань щодо пошуків нових інструментів і методів ефективної боротьби із кіберзлочинністю. А. Алієв вважає, що доречно окреслити головні виклики, які гальмують процес цифровізації публічного управління у сфері кібербезпеки, що насамперед поглибилися в обставинах війни і вимагають комплексного усунення як в коротко-, так і в довгостроковому майбутньому, зокрема:

1. «Фрагментарність цифрової інфраструктури, яка проявляється у відсутності єдиного архітектурного підходу до цифровізації державних органів, нерівномірному розвитку ІТ-рішень у міністерствах і регіонах, а також наявності застарілих або незахищених систем у сфері безпеки та оборони.

2. Низький рівень інтеграції інформаційних систем, що ускладнює оперативний обмін даними між відомствами, гальмує процес прийняття управлінських рішень у кризових умовах та створює ризики дублювання функцій або втрати важливої інформації.

3. Брак висококваліфікованих ІТ-кадрів, особливо в регіональних структурах безпеки, правоохоронних органах та підрозділах цивільного захисту. Війна спричинила як фізичне знищення частини потенціалу, так і трудову міграцію спеціалістів у приватний або закордонний сектор.

4. Нормативна неврегульованість цифрових процесів, яка стосується як захисту персональних даних, так і процедур використання хмарних технологій, електронної ідентифікації, обміну інформацією в реальному часі тощо. Наявна правова база часто відстає від швидких технологічних змін або є фрагментарною та декларативною» [3].

Відколи почалася війна, потрапила під ціль великої кількості кібератак, котрі охопили державні заклади, приватні організації й населення. Ті підприємства, котрі вважаються частиною критичної інфраструктури, в тому

числі енергетичні, телекомунікаційні, ЗМІ і фінансові компанії, теж повинні знаходитися в режимі підвищеної готовності, тому що якраз зазначені сфери нерідко вважаються головними цілями під час війни. Бізнес повинен бути готовим протистояти згаданим викликам – компанії мають дати оцінку власної готовності щодо кіберінцидентів та своєї спроможності відновити роботу.

Із 2014 р. рф активно застосовує кіберпростір в гібридній агресії проти України, деструктивно впливаючи на органи державної влади, системи управління військами і зброєю сил оборони і, крім того, на об'єкти критичної інфраструктури. Країна-агресор безперервно збільшує власний арсенал кіберзброї, яка має наступальне, розвідувальне й, крім того, підривне призначення, використання котрої здатне спричинити невиправні, незворотні руйнівні ефекти.

Наразі росія продовжує залишатися одним з головних джерел загроз національній і міжнародній кібербезпеці, котра вкрай активно втілює принцип інформаційного протиборства, оснований на поєднанні деструктивних дій в кіберпросторі й інформаційно-психологічних операцій, механізми котрої активно та повсюдно використовуються в гібридній війні проти України. Подібна деструктивна діяльність формує реальну загрозу здійснення актів кібертероризму та кібердиверсій стосовно української національної інформаційної інфраструктури.

Відтак, станом на сьогодні публічне управління у сфері забезпечення кібербезпеки України характеризується наявністю комплексу системних проблем, зумовлених як об’єктивними умовами воєнного стану та гібридної агресії РФ, так і внутрішніми управлінськими дисфункціями. Їх доцільно розглядати у взаємопов’язаних вимірах.

По-перше, інституційно-управлінські проблеми. В Україні система суб’єктів забезпечення кібербезпеки продовжує залишатися фрагментованою. Повноваження між органами публічної влади нерідко перетинаються чи не передбачають конкретно встановлених меж відповідальності, через що

ускладнюється координація дій, сповільнюється реагування на кіберінциденти і погіршується результативність стратегічного управління.

По-друге, нормативно-правові проблеми. Нормативно-правова основа в секторі кібербезпеки хоч і динамічно розвивається, проте продовжує залишатися фрагментарною і неповною. Частина законодавчих актів не гармонізована між собою, а деякі положення є не відповідними новітнім стандартам Європейського Союзу та НАТО. Недостатньо врегульованими продовжують залишатися питання відповідальності за кіберінциденти, обміну даними між державною та приватною сферою і, крім того, правові режими реагування на величезні кібератаки на тлі воєнного стану.

По-третє, кадрові та освітні проблеми. Величезною вважається проблема браку кваліфікованого персоналу в секторі кібербезпеки в органах публічної влади. Державна сфера поступається приватній за ступенем оплати праці й умовами професійного зростання, що зумовлює відтік персоналу. Система підготовки й підвищення кваліфікації держслужбовців нерідко не відповідає темпам розвитку кіберзагроз та сучасних технологій, а управлінський елемент кібербезпеки продовжує залишатися недостатнім чином провадженим в освітні програми.

По-четверте, ресурсно-фінансові проблеми. Забезпечення кібербезпеки вимагає великого фінансового, технічного й інфраструктурного потенціалу, що на тлі війни обмежені. Нерівномірність фінансування між центральним й місцевим рівнями, застаріла матеріально-технічна база певних органів влади і, крім того, залежність від технічної підтримки ззовні ослаблюють стійкість вітчизняної системи кіберзахисту.

По-п’яте, проблеми взаємодії з приватним сектором та громадянським суспільством. Механізми публічно-приватного партнерства у сфері кібербезпеки поки не стали системними. Обмін даними щодо кіберзагроз між державою і бізнесом – обмежений, що погіршує ступінь захищеності критичної інформаційної інфраструктури. В той же час ступінь кібергігієни

громадян продовжує залишатися недостатнім, а державні програми зростання цифрової обізнаності володіють фрагментарністю.

По-шосте, стратегічні та прогнозні проблеми. Публічне управління у сфері кібербезпеки переважно володіє реактивним характером, сконцентрованим на усуненні наслідків кібератак, а не на їхньому запобіганні. Недостатнім чином розвиненими вважаються механізми стратегічного прогнозування, оцінювання ризиків і сценарного планування кіберзагроз, що насамперед є критичним в обставинах безперервних постійних атак на державні інформаційні ресурси, а також об’єкти критичної інфраструктури.

Із початком повномасштабного вторгнення РФ у 2022 році у сфері публічного управління кібербезпекою України виникли якісно нові проблеми, які раніше або були відсутні, або мали другорядний характер. Вони зумовлені воєнним станом, різким зростанням інтенсивності кібератак та трансформацією функцій держави, зокрема:

1. Різке зростання масштабів і складності кібератак воєнного характеру. Повномасштабна війна зумовила перехід кібератак на стадію системної кіберкампанії, націленої на: державні реєстри й інформаційні ресурси; об’єкти критичної інфраструктури (енергетика, транспорт, зв’язок); системи військового і логістичного управління. Проблемою публічного управління виявилося те, що наявні механізми реагування розраховувалися на певні випадки, а не на безперервний кібертиск в умовах війни.

2. Перевантаження та вразливість державних інформаційних систем. Коли почалося вторгнення, постала потреба: масового переходу на віддалений вид діяльності; розвитку в екстреному режимі нових цифрових сервісів (виплати, реєстри ВПО, військовий облік); оперативного масштабування електронних послуг. Це сформувало нові вразливості, тому що рішення приймалися, коли бракувало часу, без повноцінного аудиту безпеки, через що ускладнилося контролювання ризиків на рівні публічного управління.

3. Порушення стабільності міжвідомчої координації. Обставини війни поглибили проблему асиметричної координації між органами влади, в тому

числі переважання силових структур в ухваленні рішень; обмеження горизонтальної взаємодії між цивільними органами; фрагментацію інформаційних потоків з огляду на умови секретності, що зменшило дієвість комплексного публічного управління кібербезпекою.

4. Зростання ролі міжнародної допомоги та залежність від зовнішніх партнерів. Відколи почалася війна, Україна значним чином покладається на технічну підтримку міжнародних партнерів; іноземні хмарні сервіси; консультаційне сприяння зі сторони держав Європейського Союзу та НАТО. Проблемою виявилося інституційне управління зазначеною підтримкою, а саме координування, впровадження різного роду стандартів, захист незалежності інформації і довгострокова стабільність подібних рішень.

5. Інформаційно-психологічний вимір кіберзагроз. Повномасштабна війна сполучила кіберзагрози з інформаційно-психологічними процедурами; дезінформацією і маніпуляціями у цифровій сфері; кібератаками, націленими на те, щоб підірвати довіру до держави, що показало недостатнє поєднання кібербезпеки із державною інформаційною політикою.

8. Реактивний характер управління в умовах постійної кризи. Коли розпочалося вторгнення, публічне управління в секторі кібербезпеки отримало в основному кризовий, реактивний характер. Довготермінове планування, стратегічне прогнозування й системні реформи почасти поставили на друге місце, що обумовлює ризики для післявоєнного відновлення цифрової держави.

Узагальнюючи, проблеми публічного управління у сфері забезпечення кібербезпеки України мають комплексний і системний характер та потребують цілісного реформування управлінських механізмів, гармонізації законодавства з європейськими стандартами, посилення інституційної спроможності держави й розвитку партнерських моделей взаємодії в умовах воєнних і поствоєнних викликів. Повномасштабне вторгнення трансформувало кібербезпеку з відносно автономної сфери державної політики у критично важливий елемент оборонного та кризового управління,

водночас виявивши низку нових проблем публічного управління, пов’язаних із правовою невизначеністю, кадровими втратами, перевантаженням цифрових систем, координаційними збоями та залежністю від зовнішньої підтримки.

Висновки до розділу 2

1. Проведений аналіз нормативно-правового, організаційного та інформаційно-технічного забезпечення публічного управління у сфері забезпечення кібербезпеки України свідчить про утворення комплексної, багатоступеневої системи державного реагування на новітні кіберзагрози. Нормативно-правове забезпечення створює головні принципи державної політики в секторі кібербезпеки, встановлює перелік суб’єктів, їх повноваження і процедури взаємодії і, крім того, гарантує зближення вітчизняного законодавства із міжнародними і європейськими стандартами. Організаційне забезпечення публічного управління у сфері кібербезпеки основується на функціонування системи спеціалізованих державних органів й координаційних інституцій, котрі гарантують стратегічне планування, міжвідомчу взаємодію і реагування на кіберінциденти. Інформаційно-технічне забезпечення стає інфраструктурним базисом публічного управління в секторі кібербезпеки, створюючи належні умови для діяльності державних інформаційних систем, моніторингу кіберзагроз, захисту інформаційних ресурсів та підтримки управлінських рішень.

2. Ефективність реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України доречно досліджувати в контексті сильних сторін, що утворилися останніми роками. Передусім мовиться про існування фндаментальної нормативно-правової і стратегічної основи, що формує цілі, принципи та суб’єктів державної політики в секторі кібербезпеки. Значуща перевага, крім того, - затвердження на інституційному рівні відповідальності за координування і реагування на кіберзагрози і, до того ж, нагромаджений

практичний досвід протистояння глобальним кібератакам на тлі гібридної і повномасштабної війни. Додатковий фактор зростання результативності – активне міжнародне співробітництво й допомога зі сторони стратегічних партнерів, що допомагає підвищити кіберстійкість державної сфери. Водночас реалізація механізмів публічного управління у сфері кібербезпеки супроводжується низкою системних слабких сторін. З-поміж них головними продовжують залишатися фрагментарність повноважень між різними органами влади, неналежний ступінь міжвідомчої координації і нерівномірність здійснення заходів кіберзахисту на центральному та місцевому рівнях. Великою проблемою вважається проблема браку кваліфікованого персоналу і, крім того, обмежений фінансовий та матеріально-технічний потенціал, через що ускладнюється практичне впровадження стратегічних документів та погіршується загальна ефективність державної політики в згаданому секторі. Водночас реалізація потенційних можливостей відбувається в умовах значних загроз, що негативно впливають на ефективність публічного управління у сфері кібербезпеки. Безперервні кібератаки зі сторони країни-агресора, поглиблення складності кіберзагроз із застосуванням новітніх технологій і, крім того, ризики витоку чутливих даних формують додаткове навантаження на систему публічного управління. В комплексі із недостатнім ступенем кіберкультури певних груп працівників і залежністю від іноземних технологій зазначені загрози ставлять вимогу щодо наступного покращення механізмів публічного управління і поглиблення комплексного підходу щодо гарантування кібербезпеки України.

3. Проблеми публічного управління у сфері забезпечення кібербезпеки України володіють комплексним та системним характером і вимагають цілісного реформування управлінських механізмів, узгодження законодавства із європейськими стандартами, зростання інституційної здатності держави та зростання партнерських моделей взаємодії на тлі воєнних та післявоєнних викликів. Повномасштабне вторгнення перетворило кібербезпеку з порівняно автономного сектора державної політики в критично значущу складову

оборонного й кризового управління, в той же час викривши ряд нових проблем публічного управління, що мають зв’язок з правовою невизначеністю, втратами персоналу, перевантаженням цифрових систем, координаційними збоями й залежністю від допомоги ззовні.

РОЗДІЛ 3
НАПРЯМИ ВПРОВАДЖЕННЯ ІННОВАЦІЙНИХ ІНСТРУМЕНТІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

3.1. Зарубіжний досвід публічного управління у сфері забезпечення кібербезпеки

На тлі глобальної цифровізації й динамічного зростання інформаційно-комунікаційних технологій кіберпростір трансформувався в один з головних аспектів національної безпеки країн. Збільшення числа й складності кіберзагроз, в тому числі кібератак на критичну інфраструктуру, державні інформаційні ресурси й персональна інформація людей, робить актуальною необхідність утворення результативної системи публічного управління у сфері забезпечення кібербезпеки. Провідні світові держави вже акумулювали великий практичний досвід в зазначеному секторі, що охоплює напрацювання національних кіберстратегій, покращення інституційних механізмів, введення новітніх моделей міжвідомчої координації й активну взаємодію держави із приватною сферою та громадянським суспільством.

Зарубіжний досвід публічного управління у сфері забезпечення кібербезпеки відзначається системним характером, стратегічною орієнтацією і спрямованістю на превентивне реагування на кіберзагрози. Особлива увага зосереджується на нормативно-правовому регулюванні, зростанні національних центрів кіберзахисту, введенні стандартів кіберстійкості й зростанні ступеня кіберграмотності громадян. Розгляд таких підходів – значуще джерело для пристосування найбільш вдалого управлінського досвіду до вітчизняних реалій.

В розрізі новітніх безпекових викликів, в тому числі гібридної війни і збільшення значення кіберпростору як поля міждержавного протистояння, розгляд зарубіжного досвіду публічного управління в секторі кібербезпеки стає по-особливому актуальним для України. Узагальнення й критичне

дослідження міжнародних механізмів дає змогу окреслити напрями вдосконалення вітчизняної системи публічного управління, враховуючи національні інтереси.

Насамперед варто зазначити, що «соціальний та економічний розвиток все більше залежать від швидкого та безперешкодного доступу інформації та її використання в управлінні, виробництві та сфері послуг та громадськості суб'єктів. Безперервний розвиток мережевих та інформаційних систем, включаючи аналіз даних, допомагає розвивати комунікації, торгівлю, транспорт або фінансові послуги. Будь-яке значне порушення функціонування інформаційного простору матиме вплив на економічну активність населення і його безпеку, ефективність державного сектора економіки, процеси виробництва та обслуговування, і в кінцевому рахунку – на національну безпеку. На сьогоднішній день існує ризик порушення цілісності та конфіденційності інформації, у тому числі навмисних нападів у вигляді зловмисного програмного забезпечення, злому інформаційно-телекомунікаційних систем або блокування надання послуг. Зловмисниками можуть бути як злочинні групи, що мають на меті фінансову вигоду або бути підтримані іноземними державами» [194].

Потрібно наголосити, що міжнародні організації мають велике значення в напрацюванні стандартів, регулювань та пропозицій в секторі кібербезпек та, крім того, в підтримці співробітництва між державами. До головних організацій належать:

– «ООН – в рамках ООН діють кілька програм і комітетів, які розглядають питання кібербезпеки. Один із таких – Група урядових експертів ООН з питань кібербезпеки (GGE), яка розробляє норми відповідальної поведінки держав у кіберпросторі та сприяє врегулюванню кіберконфліктів;

– Інтерпол – організація виконує важливу функцію в протидії кіберзлочинності, особливо через забезпечення координації між національними правоохоронними органами різних країн. Інтерпол організовує

операції з виявлення кіберзлочинців, сприяє тренінгам для співробітників поліції та надає технологічну допомогу;

– Європейський Союз (ЄС) – у межах ЄС кібербезпека координується через агентства та ініціативи, зокрема як вже зазначалось це – ENISA (Агентство ЄС з кібербезпеки), що працює над розробкою стандартів кібербезпеки, а також координує заходи з підготовки та реагування на кіберзагрози в усіх країнах-членах ЄС;

– НАТО – військово-політичний альянс НАТО надає важливу підтримку країнам-членам у забезпеченні кібербезпеки, особливо у контексті гібридних загроз. Центр передового досвіду з кіберзахисту НАТО в Таллінні (CCDCOE) займається дослідженнями у сфері кібербезпеки, розробляє рекомендації для членів альянсу та проводить регулярні тренування з кіберзахисту» [83].

У даному контексті варто зазначити, що «міжнародна співпраця в галузі кібербезпеки є необхідною умовою для ефективного протистояння кіберзагрозам на глобальному рівні. Успішна координація, обмін інформацією та правова допомога значно підвищують спроможність держав запобігати кіберінцидентам, розслідувати кіберзлочини та залучати кіберзлочинців до відповідальності» [179].

Як відомо, «сучасна інформаційна політика в розвинених країнах – це сукупність напрямів і способів діяльності компетентних органів держави з контролю, регулювання та планування процесів у сфері одержання, зберігання, оброблення, використання та поширення інформації. Держава регулює відповідний розподіл інформаційних ресурсів, загальні принципи інформаційної діяльності, встановлює пріоритети для забезпечення національних інтересів. Власну інформаційну політику ведуть більшість держав світу, але обсяги їхньої діяльності в цій сфері залежать від поставлених завдань і рівня зацікавленості конкретної країни в інтеграції до глобальної системи комунікації, від історичних чинників, політичного й економічного розвитку, фінансових і матеріальних ресурсів» [171]. При цьому, варто розуміти, що «забезпечення кібербезпеки є проблемою для всіх суб'єктів, які

формують національну кібербезпеку, тобто суб'єктів господарювання, що надають послуги з використанням систем ІКТ, користувачів, державних органів, а також спеціалізованих установ, що займаються кібербезпекою на операційному рівні. Тому на даний час доволі важливим є міжнародне співробітництво між державами в рамках таких організацій, як ЄС та НАТО. Ця співпраця відіграє важливу роль у боротьбі зі зростаючою кількістю інцидентів, викликаних незаконною діяльністю в інформаційному просторі, що призводить до матеріальних і репутаційних збитків» [171]. Наразі розвинені держави прогресують завдяки цілеспрямованому правовому впорядкуванню відносин в національному кіберпросторі, ухваленню потрібних законодавчих актів, здійсненню перебудови роботи органів публічної влади, котрі несуть відповідальність за вироблення і втілення кіберполітики.

Як зазначає В. Крушеніцький, «однією з найрозвиненіших є модель Сполучених Штатів Америки, яка ґрунтується на інтеграції зусиль державних, військових та приватних структур у межах уніфікованої стратегії. Основними інституціями є Департамент внутрішньої безпеки (DHS), Національне агентство з безпеки (NSA) та Командування кіберпростору США (USCYBERCOM). Ці органи забезпечують координацію заходів щодо захисту критичної інфраструктури, інформаційних систем, а також протидію зовнішньому втручанню в демократичні процеси. У США існує розвинена система стратегічних комунікацій, що забезпечує оперативне реагування на спроби дезінформації. Законодавчо закріплено принципи кібергігієни, відповідальність цифрових платформ, а також налагоджено ефективну міжвідомчу взаємодію. Особливої уваги заслуговує масштабне фінансування досліджень у сфері штучного інтелекту, який застосовується для автоматизованого аналізу інформаційних потоків, виявлення аномалій і загроз у реальному часі» [85].

Як відомо, у США одним з основних органів, який реалізує управління у секторі цифрової безпеки, є Агентство з кібербезпеки та безпеки

інфраструктури (Cybersecurity and Infrastructure Security Agency – CISA) [180], котре діє у структурі Міністерства внутрішньої безпеки (Department of Homeland Security). Сформоване 2018 року, CISA має ключове значення щодо гарантування національної стійкості до цифрових загроз, насамперед в секторі критично значущої інфраструктури, що охоплює енергетичну галузь, транспорт, фінансову систему, медичні установи, водопостачання, телекомунікації, публічне управління й інші об'єкти, від котрих залежить життєдіяльність соціуму.

Одна з основних функцій CISA – «координація діяльності федеральних, регіональних та місцевих органів влади, а також приватних компаній у запобіганні, виявленні та реагуванні на кіберзагрози. Агентство здійснює безперервний моніторинг кіберпростору через спеціалізовані платформи раннього попередження, які аналізують мільйони подій у режимі реального часу, використовуючи штучний інтелект, алгоритми машинного навчання та аналітику великих даних. Такі системи дозволяють своєчасно виявляти кібератаки, фішингові кампанії, витоки даних та інші інциденти, що можуть загрожувати національній безпеці» [180]. До того ж, «CISA реалізує ініціативу «Shield Up!», що спрямована на підвищення рівня готовності організацій до кіберінцидентів. У межах цієї програми надаються рекомендації, методичні матеріали, інструкції щодо кібергігієни, інструменти для оцінки ризиків і вразливостей систем. Агентство виступає посередником між державою і приватним сектором, створюючи партнерства з технологічними компаніями, операторами критичної інфраструктури, банками та освітніми установами. Такий формат співпраці ґрунтується на обміні інформацією про кіберзагрози, спільному моделюванні сценаріїв атак, проведенні тренувань і симуляцій» [180]. Особливу роль відіграє підхід CISA до кібербезпеки як до питання загальнонаціональної безпеки, що охоплює не тільки технологічний вимір, а також людський фактор. Агентство влаштовує освітні кампанії серед населення та службовців, займається розвитком системи зростання цифрової

грамотності і забезпечує технічну підтримку організаціям, котрі не володіють достатніми власними ресурсами для гарантування кіберзахисту.

Окрему увагу CISA приділяє «забезпеченню безпеки виборчого процесу, захисту державних реєстрів, урядових веб-ресурсів, а також реагуванню на масштабні загрози, наприклад, кібератаки з боку держав-противників або транснаціональних хакерських угрупувань. Для цього агентство співпрацює з Федеральним бюро розслідувань (FBI), Агентством національної безпеки (NSA), а також міжнародними партнерами в рамках обміну досвідом та оперативними даними» [146]. Отже, функціонування CISA в США – зразок комплексного й багатоступеневого підходу до кібербезпеки, що поєднує новітні технології, міжвідомче й міжсекторальне співробітництво, стратегічне планування і відкритість до інновацій. Згаданий досвід показує, як системна цифровізація безпекових механізмів здатна істотно збільшити захищеність держави на тлі стрімкої технологічної сфери й глобальних кіберзагроз.

Стосовно органів, котрі гарантують кібербезпеку у Європейському Союзі, то 2004 року сформували Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA), яке «надає практичні поради та рішення для державного та приватного секторів в країнах ЄС. Це включає: сприяння розробці національних стратегій; сприяння співробітництву між командами з реагування на надзвичайні ситуації та розбудови потенціалу. ENISA допомагає розробити політику та законодавство ЄС з питань мережевої та інформаційної та кібербезпеки. Щоденна робота ENISA визначається щорічною робочою програмою Агентства, яка складається щороку після широких консультацій з керівництвом та виконавчою радою ENISA» [183]. Варто зауважити, що «ENISA виконує низку критично важливих функцій. Зокрема, воно забезпечує методологічну підтримку урядам країн ЄС у розробці та реалізації національних стратегій цифрової безпеки, проводить аудити кіберстійкості цифрових систем, аналізує ризики та загрози, бере участь у розслідуванні кіберінцидентів і координує транскордонну взаємодію між органами влади, приватними компаніями та структурами критичної

інфраструктури. Агентство також організовує масштабні навчання – такі як Cyber Europe – в яких беруть участь сотні установ, що імітують реагування на масштабні кібератаки» [182]. До того ж, «ENISA тісно співпрацює з Європейською комісією, Європейською службою зовнішніх дій, національними центрами реагування на інциденти кібербезпеки (CSIRT) та іншими структурами, щоб забезпечити єдині стандарти безпеки, спільні механізми моніторингу загроз і оперативне реагування на них» [182]. В 2019 році Європейський Союз ухвалив Регламент про кібербезпеку, котрий суттєво розширив мандат ENISA та закріпив за агентством координуюче значення щодо формування Європейської рамки сертифікації кібербезпеки. Крім того, «ENISA реалізує широку просвітницьку діяльність, спрямовану на підвищення обізнаності громадян, службовців і бізнесу у питаннях цифрової гігієни, кіберзахисту, відповідального використання даних. Усі ці заходи мають на меті формування культури кібербезпеки як невід'ємного елементу європейської безпекової політики та економічної самостійності» [176].

Значне місце в політиці кібербезпеки Європейського Союзу займає концепція «цифрового суверенітету». Як відомо, «вона передбачає прагнення держав-членів до збереження контролю над національними цифровими ресурсами, зокрема, над персональними даними громадян, критично важливою інфраструктурою, державними сервісами та стратегічними технологіями. У межах цієї концепції активно розвивається ініціатива GAIA-X, яка має на меті створення європейської федеративної хмарної інфраструктури, незалежної від глобальних гігантів, таких як Amazon, Google чи Microsoft» [176].

Варто звернути увагу на те, що «стратегічна мета ЄС полягає не лише в захисті від зовнішніх загроз, а й у підвищенні автономності в розробці та використанні цифрових технологій» [178]. Зазначений підхід передбачає сприяння європейським інноваційним екосистемам, стартапам та компаніям, які провадять діяльність в галузі штучного інтелекту, IoT, хмарних обчислень, блокчейну й інших критичних векторів цифрової трансформації. Програми

Horizon Europe, Digital Europe Programme, European Defence Fund включають мільярдні інвестиції в зростання таких технологій, враховуючи високі стандарти кібербезпеки.

Європейський центр кіберзлочинності «було створено у 2013 році для посилення реагування правоохоронних органів на кіберзлочинність в ЄС і таким чином сприяє захисту європейських громадян, підприємств та урядів від злочинів в мережі Інтернет. З моменту свого створення, Європейський центр кіберзлочинності вніс значний внесок у боротьбу з кіберзлочинністю. Щороку Європейський центр кіберзлочинності публікує Оцінку загрози організованої злочинності в Інтернеті, її головний стратегічний звіт про основні висновки та нові загрози та події в сфері кіберзлочинності» [183]. 10 грудня 2018 року Європейським Парламентом та Європейською Комісією вдалося досягти політичної домовленості стосовно Закону про кібербезпеку, котрий поглиблює повноваження ENISA для того, щоб надавати кращу підтримку країнам-членам в боротьбі з загрозами в секторі кібербезпеки. Крім того, закон визначає межу Євросоюзу для сертифікації кібербезпеки, завдяки чому зростає безпека онлайнових послуг і споживчих приладів. Закон про кібербезпеку передбачає надання агентству більшого обсягу ресурсів для того, щоб воно мало можливість здійснити свої завдання; зміцнення бази для ENISA у новій системі сертифікації кібербезпеки, щоб надавати допомогу країнам-членам в дієвому реагуванні на кібератаки. Зокрема, «цілями створення такої Агенції встановлено такі: впроваджувати та розвивати високий рівень експертиз; допомагати європейським інституціям, органам, офісам і агенціям розробляти політики безпеки мереж та інформації; допомагати впроваджувати необхідні політики для досягнення необхідних вимог, встановлених існуючими та в майбутньому розробленими актами; розвивати спроможності у підготовці до упередження, виявлення та реагування на проблеми, пов'язані з безпекою мереж та інформації, підтримувати закордонну кооперацію між учасниками державних органів та приватного сектору» [183]. Практика

публічної політики кібербезпеки, яка реалізується в деяких державах Європейського Союзу охарактеризована у табл. 3.1.

Зокрема, «в рамках своєї Стратегії кібербезпеки Австрія переслідує такі стратегічні цілі: наявність, надійність і конфіденційність обміну даними, а також цілісність самих даних; віртуальний простір повинен бути здатний протистояти ризикам, поглинати удари і регулювати до зміни середовища; розробка ключових систем ІКТ; на основі національного підходу компетентних федеральних міністерств Австрія забезпечить розвиток інфраструктури ІКТ; забезпечення високого рівня доступності, цілісності та конфіденційності необхідних інфраструктур ІКТ; Австрія відіграватиме активну роль у міжнародному співробітництві» [188]. Як відомо, в Австрії була прийнята Національна стратегія безпеки інформаційно-комунікаційних технологій, якою передбачається виконання таких стратегічних цілей та заходів: «оптимізація числа зацікавлених сторін у сфері кібербезпеки в Австрії; налагодження зацікавлених сторін із інформаційною структурою; підвищення безпеки в кіберпросторі; сприяння міжнародній співпраці» [188].

У Великобританії «діє Закон про захист даних, який контролює, як особисті дані людини використовуються організаціями, підприємствами або урядом. Кожна особа, відповідальна за використання персональних даних, повинна дотримуватися суворих правил, які називаються "принципами захисту даних". Вони повинні переконатися, що інформація: справедливо, законно і прозоро використовується для визначених, явних цілей; зберігається не довше, ніж це необхідно; обробляється таким чином, що забезпечує відповідну безпеку, включаючи захист від незаконної або несанкціонованої обробки, доступу, втрати, знищення або пошкодження» [202].

Таблиця 3.1

Практика публічної політики кібербезпеки деяких держав Європейського Союзу

Країна	Характеристика	Ціль	Суб’єкти реалізації
Австрія	Національні стратегії побудовані на основі всеосяжного і	Стратегія спрямована на забезпечення безпеки	Керівна група з кібербезпеки Експертний центр з питань

	інтегрованого підходу до забезпечення інформаційної безпеки	інформаційного простору в країні	кіберзлочинності Австрійський центр кібербезпеки
Велика Британія	Національна стратегія кібербезпеки 2021 – 2026 включає набір планів, що ґрунтуються на роботі з приватним сектором	Стратегія спрямована на запобігання та зменшення впливу кібератак на Великобританію	Центр по боротьбі з експлуатацією та захисту дітей в Інтернеті Управління кібербезпеки та інформаційного забезпечення
Естонія	Національна стратегія кібербезпеки базується на комплексному підході до забезпечення інформаційної безпеки	Стратегія спрямована на полегшення використання інформаційних технологій та забезпечення їх безпеки	Управління інформаційних систем
Іспанія	Національна стратегія кібербезпеки має на меті створити адекватний потенціал для запобігання, захисту, виявлення, реагування та відновлення інформації	Стратегія спрямована на забезпечення безпеки інформаційного простору в країні та посилення її конкурентоспроможності	Національний центр розвідки Рада національної безпеки Спеціалізований комітет з кібербезпеки
Італія	Національна стратегія щодо безпеки кіберпростору є інтегрованими, структурованими та гнучкими	Стратегія спрямована на запобігання майбутнім загрозам в інформаційній сфері стабільність країни	Комітет з інформаційного суспільства Міністерство з інновацій та технологій Комітет з інформатизації держ установ
Німеччина	Національна стратегія кібербезпеки базується на комплексному підході до забезпечення інформаційної безпеки	Стратегія спрямована на підтримку та сприяння соціально-економічного розвитку Німеччини за рахунок інформаційних технологій	Офіцер захисту даних Національний центр кіберзахисту Національна рада кібербезпеки

Джерело: розроблено за матеріалами [174; 181]

У Великій Британії діє Національний центр кібербезпеки (NCSC) [200], котрий вважається головною структурою, яка здійснює координацію зусиль уряду, приватного сектору й наукового кола в секторі цифрової безпеки. В межах проєктів із кіберстійкості інтенсивно вводяться технології квантового шифрування, які гарантують захист каналів зв’язку від перехоплення і декодування на тлі зростання квантових обчислювальних потужностей. Крім того, британські урядові структури експериментують з застосуванням

predictive analytics в протидії тероризму й кіберзлочинності, коли моделі машинного навчання застосовуються з метою вивчення поведінкових шаблонів, встановлення ризиків у цифровій сфері й моделювання алгоритмів реагування. До того ж, у Великобританії схвалена Стратегія кібербезпеки, якою «визначається суттєвий набір цілей та показників з метою відображення реального стану у таких трьох аспектах, як: захист (уряд зміцнить власні засоби захисту інформації та працюватиме з промисловістю, щоб забезпечити захист британських мереж, даних і систем від кіберзагроз); утримання (Велика Британія зміцнить спроможність правоохоронних органів збільшити вартість кіберзлочинності); розвиток (уряд допоможе розвивати критичні можливості Великобританії, включаючи кібер-навички, а також зростаючу індустрію кібербезпеки країни, щоб не відставати від кіберзагроз)» [202].

Досвід Естонії, однієї з країн Балтії, «відзначається впровадженням моделі «електронної держави». В основі її – потужна кіберінфраструктура, повна цифровізація адміністративних процесів, висока якість цифрової освіти та ефективне публічно-приватне партнерство. Естонія досягла одного з найвищих рівнів цифрової ідентифікації громадян, що забезпечує не лише безпеку даних, а й довіру населення до державних електронних сервісів» [85]. Новітні технології проникли на всі рівні функціонування держави – від обміну інформацією між відомствами до участі населення у виборах в онлайн-режимі, а кібербезпека досліджується як елемент національної оборонної концепції.

Варто зазначити, що «одним із важливих елементів цієї системи є електронне управління в умовах криз, яке дозволяє органам влади швидко ухвалювати рішення, координувати дії між структурами, вести документообіг у цифровому форматі та забезпечувати безперервність публічного управління навіть у разі кіберінцидентів або фізичної дестабілізації» [175]. Централізована інфраструктура інформації, яку започатковано на платформі X-Road, дає можливість безпечним чином здійснювати обмін даними між державними структурами й реагувати на надзвичайні ситуації у реальному часі.

Окреме значення має формування так званого «кіберрезерву» – «мережі добровольців і професійних фахівців з ІТ-сфери, які можуть бути оперативно мобілізовані у випадку загроз національній кібербезпеці. Цей механізм функціонує за підтримки Кібероборони Естонії (Estonian Defence League's Cyber Unit)» [199], що вважається елементом територіальної оборони. До кіберрезерву належать аналітики, програмісти, інженери, котрі провадять тісну співпрацю із урядовими структурами, Службою інформації та безпеки Естонії і, крім того, міжнародними партнерами по НАТО.

Як зазначає А. Стельмах, «інтеграція великих баз даних, інтелектуальний аналіз ризиків і автоматизоване виявлення загроз стали невід'ємною частиною роботи силових і безпекових структур. Естонські установи використовують алгоритми машинного навчання та штучного інтелекту для аналізу аномальної активності в інформаційних системах, прогнозування потенційних атак, а також для забезпечення безпеки державних сервісів, включаючи охорону персональних даних, фінансових транзакцій, е-охорони здоров'я та е-правосуддя» [146]. При цьому, значущий елемент безпекової політики – тісна інтеграція Естонії у євроатлантичні безпекові структури, включно зі співробітництвом з НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) [201], який розміщений в Таллінні. Згаданий центр вважається провідним міжнародним середовищем досліджень і навчання у сфері кібероборони.

Досвід Естонії показує, що «цифрова трансформація системи національної безпеки може бути не лише інструментом технічного оновлення, але й основою для створення нової філософії оборони – відкритої, гнучкої, технологічної та орієнтованої на активну участь суспільства» [146]. Важливим є факт, що цифрова програма 2025 для Естонії «передбачає використання ІКТ у різних сферах життя. Кінцевою метою є збільшення економічної конкурентоспроможності, добробуту людей та ефективності державного управління» [202]. В стратегії окреслюються різноманітні заходи й дії задля здобуття зазначеної мети, в тому числі закінчення функціонування

широкосмугової мережі; в перспективі електронні послуги будуть дедалі більше транскордонними; 20% активних громадян ЄС повинні застосовувати цифрові технології; Естонія стане надавати власні безпечні послуги жителям інших держав; підтримка репутації Естонії як центру інновацій і розвитку інформаційного суспільства.

Кіберполітика Франції є «складовою державної стратегії розвитку країни, стратегії франкофонії та збереження національної самобутності й ідентичності, компонентом зовнішньої політики, участі Франції в інформаційних програмах і проектах міжурядових європейських організацій, створення інформаційної економіки та поширення комп'ютерних мереж і систем, інформаційних послуг. Французька національна стратегія кібербезпеки передбачає такі стратегічні цілі: стати кіберохороною державою у кіберзахисті; забезпечити здатність Франції приймати рішення шляхом захисту інформації, пов'язаної з її суверенітетом; посилити кібербезпеку національних інфраструктур; забезпечити безпеку в кіберпросторі» [202]. Щоб досягти окреслених цілей, встановлено 7 секторів діяльності: «ефективно передбачати та аналізувати навколишнє середовище, щоб прийняти відповідні рішення; виявляти та блокувати атаки, оповіщення та підтримку потенційних жертв; посилити наукові, технічні, промислові і людські можливості для підтримки незалежності країни; захистити інформаційні системи держави та операторів для забезпечення кращої національної стійкості; адаптувати французьке законодавство до врахування технологічних розробок і нових практик; розробити ініціативи міжнародної співпраці у сфері інформаційної системи безпеки, кіберзахисту і боротьби з кіберзлочинністю з метою кращого захисту національних інформаційних систем; спілкуватися, інформувати та переконувати, щоб збільшити розуміння населення масштабів викликів, пов'язаних з інформаційними системами безпеки» [202].

Що стосується Німеччини, то «правовою основою для формування політики кібербезпеки є Закон про посилення безпеки IT-систем від 2015 року. Цей документ закріплює визначення критичної інфраструктури (енергетика,

транспорт, охорона здоров'я тощо) та надає Федеральному відомству з безпеки у сфері IT (BSI) провідну роль у захисті державних і приватних цифрових систем. Командування стратегічної розвідки Бундесверу здійснює управління сучасними супутниковими системами SAR-Lupe та SATCOMBw, які забезпечують високоточну розвідку і безпечний зв'язок. Запровадження споживчого маркування IT-безпеки для комерційних продуктів є свідченням комплексного підходу до безпеки цифрового простору» [166]. У Німеччині ключовим принципом кібербезпеки вважається той факт, що «будь-яке використання інформації заборонено. Таким чином, заборонені зберігання, передача чи зміна інформації. Це правило не поширюється лише на те використання інформації, яке дозволене законом або зацікавленою стороною. Стратегія забезпечення кібернетичної безпеки ФРН зосереджується на десяти стратегічних напрямках: захист критично важливих кіберінфраструктур; захист IT-систем в Німеччині; посилення кібербезпеки в публічному управлінні; створення національного центру кіберреакції; утворення національної ради з кібербезпеки; проведення ефективного контролю за злочинністю у кіберпросторі; проведення ефективних скоординованих дій для забезпечення кібербезпеки в Європі і в усьому світі; використання надійних інформаційних технологій; розвиток персоналу у федеральних органах влади; інструменти для реагування на кібератаки» [174].

В Ізраїлі впроваджується концепція активного кіберзахисту, яка включає не тільки оборону, а також превентивні заходи. Тісне об'єднання армії, спецслужб, наукових інститутів та стартапів гарантує напрацювання розроблення інноваційних рішень, що дають змогу результативно захищати інфраструктуру критичну характеру. Зокрема, «сучасна інфраструктура кібербезпеки в Ізраїлі охоплює приблизно 450 компаній, включно з відомими фірмами, такими як «Check Point», а також численні стартапи та венчурні фонди, зокрема «Jerusalem Venture Partners (JVP) Cyber Labs», що активно інвестують у цю галузь. Крім того, значну роль відіграють науково-дослідні проєкти, які сприяють співпраці між високотехнологічними компаніями та

дослідницькими центрами» [40]. В червні 2018 р. Ізраїльський національний кібердиректорат (INCD) здійснив оприлюднення проєкту закону про кібербезпеку для обговорення громадськістю. Згаданий проєкт закону орієнтований на те, щоб регулювати функціонування INCD згідно з рішеннями уряду, і вважається завершальним етапом формування національної кібербезпекової структури. Документ включає 3 головні розділи:

1) «організаційний розділ визначає структуру та організаційні аспекти INCD;

2) оперативний розділ описує повноваження щодо виявлення та реагування на кібератаки;

3) регуляторний розділ встановлює національні та секторальні регуляції, спрямовані на підвищення стійкості різних секторів і визначає роль INCD як національного регулятора у сфері кібербезпеки» [40].

Варто зауважити, що «в Ізраїлі кібербезпека – це частина національної стратегії виживання, враховуючи складне геополітичне положення держави. Основний акцент робиться на проактивному виявленні загроз через системи прогнозної аналітики, що базуються на великих обсягах даних. Ці системи дозволяють виявляти підозрілу активність задовго до того, як вона переросте у повномасштабний інцидент. Ізраїль також є одним із лідерів у використанні блокчейн-технологій для захисту урядових баз даних, що забезпечує децентралізований контроль, прозорість доступу до інформації та підвищену стійкість до кібервтручання. Крім того, в країні активно розвиваються інструменти кібервоєнної стратегії – як оборонні, так і наступальні – у рамках діяльності таких підрозділів, як Unit 8200» [203]. Іншими словами, ізраїльська модель кібербезпеки – яскравий зразок дієвого поєднання державної політики, технологічного зростання й стратегічного мислення. Вона основується на активному, а не реактивному підході до кіберзагроз, що дає змогу Ізраїлю не тільки оперативно відповідати на атаки, а також йти на випередження ймовірним загрозам.

За висловлюванням іноземних вчених, «Національна стратегія кібербезпеки є стратегічним документом, що надає іспанському уряду основу для розробки положень Стратегії національної безпеки з метою забезпечення запобігання кіберзагроз, захисту, виявлення, реагування та відновлення інформаційного простору. Стратегія складається з п'яти розділів. Перший «Кіберпростір і його безпека», окреслює характеристики, які визначає кіберпростір. Цей розділ показує, як особливі характеристики, які є спільними для кіберзагроз призводять до збільшення ризиків, які можуть мати серйозний вплив на національну безпеку. Другий розділ стосується мети та керівних принципів кібербезпеки в Іспанії. У третій главі Стратегія більш детально розглядає цілі кібербезпеки. Четвертий розділ визначає дії, спрямовані на забезпечення національної кібербезпеки. П'ятий розділ присвячений питанням кібербезпеки в системі національної безпеки і встановлює організаційну структуру служби кібербезпеки» [181].

Що стосується Італії, «при виробленні основних положень кіберполітики уряд визначив пріоритетами трансформацію органів державного урядування на основі інформаційно-комунікаційних технологій, вільний доступ для громадян і підприємців, реалізацію електронної освіти для державних службовців, прозорість державного документообігу за допомогою Інтернету, забезпечення якості інформаційних продуктів і послуг. Виконання поставлених цілей контролюється Національним центром з питань інформатики при Державній адміністрації» [172]. У 2013 році в Італії була прийнята національна стратегія кібербезпеки. Серед завдань національної стратегії визначено: «підвищення технічного, оперативного та аналітичного досвіду всіх зацікавлених сторін та установ шляхом спільних зусиль та узгодженого підходу; зміцнення потенціалу для захисту критично важливих національних інфраструктур та стратегічних активів та зацікавлених сторін; сприяння та заохочення культури кібербезпеки; посилення можливостей протидії онлайн-злочинної діяльності, шкідливої та незаконної діяльності; посилення міжнародного співробітництва» [172]. Крім цього, «в Італій

ухвалено Національний план із захисту кіберпростору та безпеки інформаційно-комунікаційних технологій. Цей Національний план визначає оперативні керівні принципи, цілі до яких переслідувати та напрямки дій, які необхідно здійснити, щоб забезпечити повну реалізацію до національної стратегії безпеки кіберпростору» [172].

Щодо досвіду Польщі, то «основне завдання у справі забезпечення кібернетичної безпеки покладено на Агентство внутрішньої безпеки (ABW). Ним 2013 року було здійснено розробку Стратегії кібербезпеки Польщі, крім того, Агентство виступило з ініціативою створити Центр криптології при Міністерстві національної оборони, що має захищати інформацію, здійснювати кібероборону й вести наступальні кібероперації» [132]. При цьому, «ABW також створило урядову команду реагування на комп'ютерні інциденти (CERT), головним завданням якої є «забезпечення і розвиток можливостей органів публічного управління щодо захисту від кіберзагроз, зокрема від атак на інфраструктуру, що складається з IT-систем та комп'ютерних мереж, порушення роботи або руйнація яких може значною мірою загрожувати життю і здоров'ю людей, національним багатствам та навколишньому середовищу або призвести до значних фінансових збитків і збоїв у функціонуванні органів державної влади». Оскільки зросли інформаційні гібридні загрози, що, приміром, мають ознаки пропаганди, дезінформації або психологічного залякування, які здійснюють інші держави й недержавні виконавці (терористичні та інші організації), Бюро національної безпеки Польщі (BBN) 2015 року взялося за розроблення національної Доктрини інформаційної безпеки» [132]. Аби протистояти тенденціям негативного характеру, рекомендується розпізнавати інформаційну сферу, зокрема встановлювати дружні, нейтральні та ворожі суб'єкти. Концепцією польської кібербезпеки є виконавчий документ, котрий має Стратегія національної безпеки.

Варто звернути увагу на те, що «польські політичні еліти давно зрозуміли важливість побудови міцної системи кіберзахисту і перейшли до

дій. В останні роки Польща демонструє послідовну державну політику боротьби із кіберзагрозами. Польща усвідомила небезпеку кіберзагроз після масштабних кібератак 2012 року. Тоді була паралізована робота урядових сайтів, а масові протести, що почалися на вулицях, прокотилися і в мережі шляхом масованих кібератак. Через це, Польща ухвалила зміни до законодавства, які дозволяють запроваджувати у країні надзвичайний стан в разі атаки у віртуальному просторі» [187]. Наразі Польща націлює свої заходи на безпеку і надійність інформаційно-комп'ютерних технологій і остерігається зловживань і порушень – і водночас погоджується з потребою захисту відкритості й свободи інтернету. Формулювання Стратегії кібербезпеки містить таке: «Кібербезпека повинна бути вільною від небезпек або збитків, спричинених порушенням або випаданням ІКТ або зловживанням ІКТ. Вони можуть включати обмеження доступності та надійності ІКТ, порушення конфіденційності інформації, що зберігається в ІКТ, або пошкодження цілісності цієї інформації» [187].

В Австралії цифрова трансформація системи національної безпеки втілюється за допомогою Australian Signals Directorate (ASD) [173], що має головне значення щодо напрацювання засобів цифрової оборони. Держава динамічно вводить кіберрозвідку, сформовану відповідно до принципів прогнозного моделювання, вивчення кіберповедінки й оцінки вразливостей цифрової інфраструктури. Австралійський уряд вкладає інвестиції в національні дослідницькі програми в секторі квантових технологій, в тому числі організацію центрів квантового шифрування задля захисту державних даних від потенційних загроз зі сторони суперкомп'ютерів. Велику увагу надають міжнародному співробітництву, в тому числі у межах Five Eyes – альянсу розвідслужб, який, крім того, охоплює США, Великобританію, Канаду і Нову Зеландію.

Технологічні інструменти і стратегії захисту від кіберзагроз – значущий елемент системи кібербезпеки, який гарантує захист інформаційних систем, мереж та інформації. Зважаючи на динамічне зростання технологій та

безперервно зростаючий ступінь складності кібератак, держави й організації повинні весь час здійснювати оновлення своїх технологічних засобів і пристосовувати стратегії захисту для протидії новим загрозам. Зокрема, серед зарубіжних країн системи ідентифікації та управління доступом є «ключовими інструментами, що дозволяють контролювати доступ користувачів до критичних ресурсів та інформаційних систем. Сучасні системи IAM використовують багатофакторну аутентифікацію (MFA), що значно знижує ризик несанкціонованого доступу до мереж. Біометричні технології, такі як розпізнавання відбитків пальців, сканування райдужної оболонки ока та розпізнавання обличчя, забезпечують додатковий рівень захисту, роблячи процес аутентифікації більш надійним» [83].

Підбиваючи підсумки, зазначимо, що всі проаналізовані підходи до забезпечення кібербезпеки показують значущість комплексного, стратегічного й динамічного підходу до захисту національного кіберпростору. Їхній розгляд дає можливість виділити позитивні складові, котрі Україна може адаптувати:

1. Гармонізація нормативно-правового забезпечення, у контексті чого рекомендується привести у відповідність українські норми за зразком європейських стандартів (NIS2), з метою полегшення інтеграції до єдиного цифрового ринку.

2. Інституційний аспект, у контексті якого рекомендується створити єдиний національний координаційний центр з питань кібрбезпеки з міжвідомчим статусом (США).

3. Забезпечення безпечного електронного урядування, у конеткслі чого рекомендується впровадити єдину цифрову ідентифікацію громадян та захистити державні онлайн-сервіси.

4. Оптимізація цифрової освіти, у контексті чого рекомендується масштабувати програми цифрової грамотності, внести теми кібербезпеки у навчальні курси кожного рівня освіти (країни Європейського Союзу).

5. Посилення міжнародної кооперації, у контексті чого рекомендується розширити участь в міжнародних кіберструктурах, здійснювати обмін інформацією, організовувати спільні тренування та круглі столи.

6. Посилення кадрової підготовки, у контексті чого рекомендується створити кіберрезерв, здійснювати підтримку ІТ-освіти та розвивати співпрацю держави, університетів і бізнесу (Ізраїль).

7. Забезпечення громадського контролю, у контексті чого рекомендується забезпечити прозорість державної політики, підвищити інклюзивність процесів і залучити громадянське суспільство до процесу забезпечення кібербезпеки.

Розгляд і узагальнення міжнародного досвіду стосовно створення й втілення механізмів гарантування публічної політики кібербезпеки, давши можливість напрацювати головні вектори зростання певних національних механізмів в Україні, зокрема: гарантування доступу до інформації; формування національних кібернетичних ресурсів; застосування інформаційних ресурсів у національних цілях; формування загальної системи охорони інформації; підтримка міжнародної взаємодії в секторі комунікації, а також інформації; забезпечення інформаційного державного суверенітету; зростання кібернетичної інфраструктури.

3.2. Шляхи удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України

Сучасна фаза становлення української держави відзначається динамічною цифровізацією публічного управління, збільшенням значення інформаційно-комунікаційних технологій і зростанням залежності критично значущих секторів життєдіяльності від сталого функціонування кіберпростору. На тлі повномасштабної збройної агресії рф проти України кіберпростір виявився повноцінною ареною протиборства, а кібератаки стали засобом дестабілізації систем державного управління, економіки, оборони й

безпеки суспільства. В таких умовах гарантування відповідного ступеня кібербезпеки отримує статус одного із основних пріоритетів державної політики і національної безпеки України.

Водночас діюча система публічного управління у сфері кібербезпеки відзначається рядом проблем, з-поміж котрих фрагментарність нормативно-правового регулювання, недостатній рівень координації між суб'єктами сфери безпеки й оборони, обмеженість інституційної здатності органів публічної влади і, крім того, нерівномірність готовності об'єктів критичної інфраструктури протидіяти новітнім кіберзагрозам. Існуючі механізми публічного управління нерідко не адекватні темпам зростання кіберзагроз, що спричиняє необхідність їхнього комплексного перегляду й пристосування до нової безпекової реальності.

В згаданому аспекті особливо актуальним стає пошук шляхів удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України, націлених на збільшення результативності державної політики, зростання міжвідомчої взаємодії, введення ризик-орієнтованого підходу й застосування найбільш вдалого міжнародного досвіду. Комплексне оновлення нормативно-правових, організаційних, інформаційно-технічних механізмів повинне бути основою для утворення сталої національної системи кібербезпеки, що здатна результативно функціонувати в обставинах воєнних та поствоєнних викликів і гарантувати захист національних інтересів України в кіберпросторі.

В. Рядінська, досліджуючи нормативно-правове забезпечення цифровізації публічного управління, зазначає, що після того, як прийнято DSMS, та донині правове регулювання цифровізації в секторі публічного управління у ЄС визначає, що у державах Європейського Союзу законодавство має утворюватися так, щоб визначати вимоги і єдині стандарти стосовно:

– «захисту персональних даних, які повинні виконувати всі суб'єкти (в тому числі і органи публічної адміністрації), які працюють з персональними даними громадян ЄС відповідно до вимог GDPR;

– забезпечення доступності веб-сайтів і мобільних застосунків органів публічної адміністрації для інвалідів та інших категорій маломобільних осіб населення(инклюзивность цифровізації) (відповідність WCAG 2.1);

– створення умов для функціонування норми загальноєвропейського єдиного цифрового порталу (SDG), який дає змогу отримувати державні послуги в електронному вигляді в будь-якій країні ЄС;

– забезпечення вимог кібербезпеки в діяльності органів публічної адміністрації (відповідно до вимог NIS2, Cybersecurity Act), взаємного визнання цифрових ідентифікаторів (відповідність eIDAS);

– впровадження механізмів для реалізації принципу Once-Only Principle (надання інформації лише один раз) шляхом забезпечення автоматичного обміну інформацією між національними реєстрами без необхідності повторного введення даних;

– доступність електронних державних послуг в будь-якій країні ЄС для іноземних користувачів (фізичних та юридичних осіб ЄС);

– забезпечення багатомовності цифрових державних сервісів (наявність інтерфейсу однією з офіційних мов ЄС, окрім національної мови країни, або автоматичного перекладу);

– стимулювання розвитку Інтернету речей (IoT);

– забезпечення права користувачів змінювати провайдерів без втрати доступу до державних сервісів; сприяння використання відкритих даних державного сектору, створення державними органами своїх даних відкритими, стандартизованими та доступними онлайн» [139].

Т. Станіславський зазначає, що необхідно виконати такі заходи для удосконалення публічного управління у сфері забезпечення кібербезпеки України:

1. «Розвиток організаційних механізмів. Механізм має бути осучасненим і відповідати принципам стратегічного планування на ланці суб'єкти кібербезпеки – національний координатор – Уряд. При цьому, визначальну роль в координації діяльності суб'єкта кібербезпеки (незалежно від його відомчої або галузевої приналежності) має бути відповідальна за безпеку мереж та інформації посадова особа з числа керівництва (заступник керівника) такого суб'єкта. В її обов'язках має бути чітко визначена роль, задачі, функції та відповідальність за зазначену сферу суб'єкта кібербезпеки, враховуючи його невід'ємну частину – стратегічне та поточне планування та їх бюджетування. Координуюча роль Центру має бути посилена завданням з організації та координації діяльності всіх суб'єктів кібербезпеки з стратегічного та поточного планування і схвалення проектів планів заходів на три роки та на рік. Уряд має затверджувати вимоги з формування, оформлення та подання пропозицій стратегічного та бюджетного планування заходів з реалізації стратегії та забезпечення кібербезпеки та лише забезпечувати заплановані заходи в частині організації планування на відповідний період. Держспезв'язку має узагальнювати пропозиції всіх суб'єктів кібербезпеки вносити їх на розгляд Центру та, в подальшому, вносити до Кабінету Міністрів України.

2. Розвиток правових механізмів. Положення про Національний координаційний центр кібербезпеки має бути доповнено нормами щодо координуючої функції в стратегічному та поточному плануванні заходів з реалізації стратегії та інших заходів забезпечення кібербезпеки, з наданням можливості оперативного реагування на зміни у кіберпросотрі, що суттєво впливають на стан кібербезпеки. Положення про центральні органи виконавчої влади, які у доручених сферах мають об'єкти критичної інфраструктури, мають бути доповнені завданнями щодо кібербезпеки та кіберзахисту таких об'єктів, подання інформації щодо переліків таких об'єктів, стану та спроможності цих суб'єктів забезпечити кіберзахист об'єктів критичної інформаційної інфраструктури тощо. В типовій структурі

центральних органів виконавчої влади мають бути уведені структурні одиниці, що відповідатимуть за організацію роботи щодо кібербезпеки та кіберзахисту як об'єктів критичної інфраструктури у відповідній галузі так і безпеки мереж та інформації в самому державному органі, розроблення та впровадження дієвих механізмів забезпечення конкретності заходів, їх відповідності основним цілям стратегії, вимірюваності результатів заходів та спроможності їх виконання у встановлений період та бюджетування» [145].

У свою чергу Д. Мялковський зазначає, що головними векторами щодо удосконалення діючих організаційно-правових механізмів публічного управління міжнародною співпрацею України на загальнодержавному рівні, крім того, є:

– «визначення вимог та механізмів публічного управління та адміністрування міжнародним співробітництвом у сфері кібербезпеки в умовах повсякденної діяльності та розвитку, а також надзвичайного та воєнного стану, надзвичайних ситуацій, особливого періоду;

– розроблення терміносистеми з питань кібербезпеки на основі узагальнення та систематизації вітчизняного законодавства та його гармонізації з міжнародним законодавством;

– перегляд змісту завдань щодо кібербезпеки органів, що існують, та утворення координаційного ЦОВВ з покладанням на нього одним із головних завдань координацію органів виконавчої влади з питань міжнародного співробітництва у сфері кібербезпеки;

– забезпечення взаємодії Національного центру оперативно-технічного управління мережами телекомунікацій з аналогічними центрами НАТО та ЄС, а також можливе його перепідпорядкування Міноборони з метою підвищення ефективності функціонування національної системи забезпечення кібербезпеки, особливо в умовах надзвичайних ситуацій, надзвичайного стану, воєнного стану, особливого періоду;

– створення системи моніторингу та оцінювання якості державного управління міжнародним співробітництвом України» [100].

Такі науковці, як А. Семенченко, В. Плескач, О. Заярний та М. Плескач пропонують наступні заходи удосконалення організаційно-правових механізмів публічного управління забезпеченням кібербезпеки та кіберзахисту України:

1. «Необхідно забезпечити одночасну розробку та взаємоузгоджені за змістом зміни до Закону України «Про основні засади забезпечення кібербезпеки України» [129] та проекту Закону України «Про об'єкти критичної інфраструктури та їх захист» [127].

2. Внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України» [129] щодо його деталізації та конкретизації механізмів реалізації шляхів державно-приватного партнерства в сфері кібербезпеки та проведення оглядів кібербезпеки та кіберзахисту.

3. Відповідно до п. 4 ст.10 Закону України «Про національну безпеку України» [126.] передбачити розробку «Білої книги кібербезпеки», не рідше ніж раз на три роки, а також перенести цю норму в нову редакцію Закону України «Про основні засади забезпечення кібербезпеки в Україні» [129].

4. Розробити та прийняти порядок проведення «оглядів національної системи кібербезпеки» та «огляду стану кіберзахисту державних інформаційних ресурсів та критичної інформаційної інфраструктури».

5. Адаптувати національне законодавство у сфері забезпечення кібербезпеки до міжнародного, насамперед, до NIS Директиви (The Directive on security of network and information systems).

6. Утворити у судах загальної юрисдикції України спеціальні колегії з розгляду справ, пов'язаних із розгляду ІТ-спорів та питаннями, пов'язаними із кібербезпекою.

7. Розробити та прийняти проект Державної цільової програми з розвитку кібербезпеки.

8. Гармонізувати міжнародні стандарти в сфері кібербезпеки.

9. Здійснити кодифікацію, розробити та прийняти Інформаційний кодекс України (Кодекс України про інформацію).

10. Забезпечити адаптацію наявної інфраструктури державних установ до вимог кібербезпеки, насамперед у частині роботи державних службовців із електронними засобами (е-пошти тощо), стаціонарного та мобільного зв'язку, користування відкритим сегментом глобальної мережі Інтернет.

11. Розробити механізм проведення регулярного аудиту об'єктів критичної інфраструктури та програми кібернавчання публічних службовців, уповноважених посадових осіб підприємств - адміністраторів публічних реєстрів, інформаційних систем.

12. Розробляти, впроваджувати, оновлювати різні освітні програми у закладах вищої освіти щодо кібербезпеки та кібергігієни з проведенням круглих столів, міжнародних конференцій, симпозіумів.

13. Стимулювати розвиток програм державно-приватного партнерства у сфері забезпечення кібербезпеки, включаючи аспекти оновлення національної інформаційної інфраструктури, за винятком критичної» [141].

Щоб усунути опір певним змінам в діяльності службовців, може стати в нагоді послідовна зміна світогляду й поетапність в діяннях. Водночас існує потреба гарантування справедливого захисту інтересів і прав усіх сторін, які в цьому закавлені. Такими третіми сторонами можуть стати приватні, громадські чи навіть публічні органи, проте вони повинні бути незалежними в юридичному й операційному аспектах і вважатися саме такими. Вони мають змогу з перевагами здійснювати певні з таких завдань:

– «погодити та оприлюднити громадянську хартію прав та обов'язків користувачів щодо використання публічних даних та громадської участі, покладаючись на те, що вже є у законі чи нормативно-правових актах, та відкрити це для обговорення користувачами та внесення змін;

– визначити та впровадити рамки для реальної мотивації, стимулювання та винагороди користувачів за залучення до розробки послуг та участі у політиці;

– постійно контролювати потенційні ризики та інформувати користувачів про них, а також пропонувати можливі рішення та допомогу;

– за запитом, та якщо доцільно, забезпечувати як проактивну, так і пасивну модерацію Web 2.0 медіа, а також нейтрально і врівноважено допомагати у проведенні рамкових дебатів;

– відстежувати та підтримувати права користувачів на конфіденційність та захист даних у відносинах з урядом та інших їхніх інтересів;

– забезпечувати, щоб всі публічні послуги ідентифікувались за походженням даних та інших використаних джерел, водночас дотримуючись вимог до відкритого джерела щодо відповідної власності та відповідальності. Це має також включати функції моніторингу та перенаправлення для забезпечення того, щоб будь-яка служба, розроблена для громадського використання, відповідала узгодженим стандартам точності та якості;

– незважаючи на величезні потенційні вигоди від звільнення всіх типів публічних даних, існує небезпека перевантаження даних та нецільового використання даних. Дані, як і статистика, можуть бути серйозно зіпсовані з метою, щоб вони означали будь-що, чого бажає будь-хто. Довірена третя сторона має відстежувати це та надавати нейтральні та прозорі настанови, а також втручатися в такі питання» [82].

Таким чином, довіра, прозорість і підзвітність виявляються найбільшими викликами сьогоднішніх реалій, які постають перед вдалим електронним урядом, й всі вони перебувають у нерозривному зв’язку. На тлі глобалізації складнішими стають не лише економічні й публічні взаємини, певну своєрідність отримують також заходи стосовно гарантування кібербезпеки.

У попередньому підрозділі було виявлено ряд проблем у кожному з механізмів публічного управління у сфері забезпечення кібербезпеки України. Зважаючи на це, на рис. 3.1. наведено комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України.

КОМПЛЕКСНИЙ МЕХАНІЗМ УДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Мета: удосконалення публічного управління у сфері забезпечення кібербезпеки України є формування цілісної, адаптивної та стійкої системи публічного управління кібербезпекою, здатної забезпечити належний рівень захисту національних інформаційних ресурсів, критичної інформаційної інфраструктури та суспільних інтересів від сучасних і перспективних кіберзагроз шляхом удосконалення нормативно-правових, організаційних та інформаційно-технічних інструментів управління.

Принципи реалізації: системності та цілісності; узгодженості та координації; законності та нормативної визначеності; адаптивності та гнучкості; ризик-орієнтованості та превентивності; інтеграції з європейськими та міжнародними стандартами; ієрархічності та субсидіарності; кіберстійкості та безперервності управління; балансу між безпекою та правами людини.

Напрями удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки

Нормативно-правовий механізм:	провести системну ревізію чинного законодавства; сформувати чітку ієрархію нормативно-правових актів; законодавчо уточнити компетенції СБУ, ДССЗЗІ, НКЦК при РНБО, Нацполіції та Мінцифри; закріпити провідного координатора; адаптувати законодавство до директив ЄС (NIS2), стандартів НАТО, ISO/IEC; запровадити механізм регулярного правового моніторингу; запровадити гнучкі правові механізми; регулярно оновлювати законодавство у сфері застосування штучного інтелекту, хмарних сервісів, Big Data; розробити спеціальні норми щодо публічно-приватного партнерства у сфері кібербезпеки; визначити стимули для приватного сектору; уніфікувати правові алгоритми реагування на кіберінциденти; закріпити стандарти кризового управління та міжвідомчої взаємодії та ін.
Організаційний механізм:	оптимізувати організаційну структуру системи кібербезпеки; чітко закріпити функції і зони відповідальності суб'єктів публічного управління; створити єдину централізовану систему координації; уніфікувати процедури міжвідомчої взаємодії; удосконалити систему підготовки та перепідготовки кадрів; сформувати механізми мотивації й утримання висококваліфікованих фахівців; нарощувати ресурсний потенціал забезпечення кіберпідрозділів; запровадити єдину систему стратегічного та оперативного планування у сфері кібербезпеки; інституціоналізувати ризик-орієнтований підхід; сформувати регіональні координаційні механізми кібербезпеки та ін.
Інформаційно-технічний механізм:	модернізувати інформаційно-технічну інфраструктуру органів публічної влади; оновити програмно-апаратні комплекси; розробити та впровадити єдині технічні стандарти і протоколи інформаційної взаємодії; уніфікувати програмно-апаратні рішення; запровадити автоматизовані системи збору, аналізу та обробки даних про кіберінциденти; цифровізувати управлінські процеси; удосконалити інформаційно-аналітичні системи моніторингу кіберзагроз; впровадити технології аналізу великих даних і кореляції подій; посилити криптографічний та технічний захист інформації; удосокналити систему резервного копіювання та відновлення даних та ін.

Очікувані результати: формування цілісної та узгодженої системи публічного управління кібербезпекою; підвищення ефективності координації та міжвідомчої взаємодії; зміцнення кіберстійкості держави та критичної інформаційної інфраструктури; підвищення рівня правової визначеності та адаптивності регулювання; посилення інформаційно-технічних та аналітичних спроможностей; активізація публічно-приватного та міжнародного співробітництва; підвищення готовності до реагування на гібридні та воєнні кіберзагрозию

Рис. 3.1. Комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України

Джерело: власна розробка автора

Метою комплексного механізму удосконалення публічного управління у сфері забезпечення кібербезпеки України є формування цілісної, адаптивної та стійкої системи публічного управління кібербезпекою, здатної забезпечити належний рівень захисту національних інформаційних ресурсів, критичної інформаційної інфраструктури та суспільних інтересів від сучасних і перспективних кіберзагроз шляхом удосконалення нормативно-правових, організаційних та інформаційно-технічних інструментів управління.

Для того, щоб побудувати комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України доцільним є виокремлення системи принципів, за допомогою яких відображається сукупність загальних засад публічного управління та специфіка кібербезпекової сфери. Принципи реалізації комплексного механізму удосконалення публічного управління у сфері кібербезпеки України включають:

1. Принцип системності та цілісності. Визначає дослідження публічного управління кібербезпекою як єдиної взаємопов’язаної системи, в рамках котрої нормативно-правові, організаційні й інформаційно-технічні складові функціонують узгодженим чином і один одного взаємодоповнюють.

2. Принцип узгодженості та координації. Націлений на гарантування конкретного розмежування повноважень та відповідальності між суб’єктами публічного управління і, крім того, результативної міжвідомчої, міжрівневої і міжсекторальної координації під час втілення державної політики кібербезпеки.

3. Принцип законності та нормативної визначеності. Визначає виконання управлінських рішень та дій тільки у рамках чинного законодавства з паралельним гарантуванням чіткості, прогнозованості й сталості правового регулювання в секторі кібербезпеки.

4. Принцип адаптивності та гнучкості. Визначає спроможність механізму публічного управління миттєво відповідати на активні зміни

кіберзагроз, технологічного зростання й безпекової сфери, передусім в обставинах воєнного стану і гібридних загроз.

5. Принцип ризик-орієнтованості та превентивності. Націлений на пріоритетність передбачення, оцінки і зведення до мінімумум кіберризиків і, крім того, на переспрямування управління із реактивних заходів на превентивні і проактивні дії.

6. Принцип інтеграції з європейськими та міжнародними стандартами. Визначає узгодження вітчизняних підходів до публічного управління кібербезпекою із директивами Європейського Союзу, стандартами НАТО й міжнародним досвідом, що допомагає збільшити сумісність і міжнародну довіру.

7. Принцип ієрархічності та субсидіарності. Визначає оптимальний синтез централізованого управління із передачею повноважень на регіональний та місцевий рівні згідно з їхніми спроможностями та відповідальністю.

8. Принцип кіберстійкості та безперервності управління. Націлений на гарантування спроможності системи публічного управління зберігати функціональність, здійснювати відновлення й пристосовуватися в обставинах кібератак, кризових ситуацій та воєнних дій.

9. Принцип балансу між безпекою та правами людини. Визначає потребу сполучення заходів кіберзахисту із додержанням конституційних прав та свобод людини, принципів демократичного врядування й верховенства права.

Зокрема, у табл. 3.2 наведено пропозиції щодо усунення проблем нормативно-правового забезпечення публічного управління кібербезпекою України.

Таблиця 3.2

Пропозиції щодо усунення проблем нормативно-правового забезпечення публічного управління кібербезпекою України.

№	Проблема	Пропозиції щодо усунення	Відповідальні органи публічної влади	Можливі перешкоди

1	Фрагментарність та несистемність нормативно-правової бази	Провести системну ревізію чинного законодавства; сформувати чітку ієрархію нормативно-правових актів	Верховна Рада України, Рада національної безпеки і оборони України, Кабінет Міністрів України, Мін'юст	Наявність високої складності координації; політичних ризиків; дублювання інтересів відомств
2	Нечіткість розмежування повноважень суб'єктів управління	Законодавчо уточнити компетенції СБУ, ДССЗЗІ, НКЦК при РНБО, Нацполіції та Мінцифри; закріпити провідного координатора	Верховна Рада України, Рада національної безпеки і оборони України, Кабінет Міністрів України	Наявність інституційної конкуренції; опору під час перерозподілу повноважень
3	Недостатня гармонізація з міжнародними та європейськими стандартами	Адаптувати законодавство до директив ЄС (NIS2), стандартів НАТО, ISO/IEC; запровадити механізм регулярного правового моніторингу відповідності	Мінцифри, Міністерство закордонних справ України, Рада національної безпеки і оборони України, профільні комітети Верховної Ради України	Наявність обмежених кадрових ресурсів; нерівномірність етапів реалізації заходів на шляху до євроінтеграції
4	Відставання правового регулювання від технологічного розвитку	Запровадити гнучкі правові механізми; регулярно оновлювати законодавство у сфері застосування штучного інтелекту, хмарних сервісів, Big Data	Мінцифри, Верховна Рада України	Наявність технологічних перешкод; дефіциту експертного середовища
5	Обмежена регламентація публічно-приватного партнерства	Розробити спеціальні норми щодо публічно-приватного партнерства у сфері кібербезпеки; визначити стимули для приватного сектору	Кабінет Міністрів України, Мінекономіки, Мінцифри, Рада національної безпеки і оборони України	Наявність недовіри бізнесу; ризиків витоку чутливої інформації
6	Недостатня деталізація процедур реагування на кіберінциденти	Уніфікувати правові алгоритми реагування на кіберінциденти; закріпити стандарти кризового	Рада національної безпеки і оборони України, Державна служба спеціального зв'язку та захисту інформації,	Наявність бюрократії; відсутність єдиних технічних стандартів

		управління та міжвідомчої взаємодії	Служба безпеки України, Кабінет Міністрів України	
7	Неврегульованість кібербезпеки на регіональному та місцевому рівнях	Розробити типові положення щодо кібербезпеки для органів місцевого самоврядування; делегувати окремі повноваження у сфері кіберзахисту	Кабінет Міністрів України, Мінрегіон, органи місцевого самоврядування	Обмеженість фінансових ресурсів громад; недостатність цифрової компетентності службовців
8	Обмеженість правових інструментів в умовах воєнного стану	Запровадити спеціальний правовий режим управління кібербезпекою під час воєнного стану; на рівні законодавства розширити повноваження кризових центрів	Верховна Рада України, Президент України, Рада національної безпеки і оборони України	Відсутність балансу між безпекою і правами людини; наявність правових ризиків як результат надмірної централізації

Джерело: власна розробка автора

Насамперед проблема фрагментарності та несистемності нормативно-правової бази вказує на неіснування цілісного підходу до регулювання кібербезпеки в правовому аспекті. Рекомендований системнй огляд діючого законодавства й утворення чіткої ієрархії нормативно-правових актів орієнтовані на те, щоб ліквідувати дублювання норм та суперечностей між ними. В той же час залучення багатьох центральних органів влади до цього процесу спричиняє значні ризики ускладненої міжвідомчої координації, політичної залежності рішень і конкуренції інституційних інтересів.

Нечіткість розмежування повноважень між суб’єктами публічного управління – одна з найбільших критичних проблем, тому що має прямий вплив на результативність реагування на кіберзагрози. Уточнення компетенцій головних органів на рівні законодавства і встановлення провідного координатора дасть можливість покращити узгодженість управлінських дій. Водночас здійснення зазначених заходів здатне зіткнутися з інституційним опором та небажанням певних органів позбуватися частини своїх повноважень.

На особливу увагу заслуговує проблема недостатньої гармонізації національного законодавства з міжнародними та європейськими стандартами. Пристосування до директив Євросоюзу, стандартів НАТО і ISO/IEC – необхідна передумова інтеграції України до безпекової сфери Європи. Введення механізму систематичного правового моніторингу адекватності буде сприяти стабільності згаданого процесу, проте його роблять складнішим обмежений кадровий потенціал і нерівномірність імплементації євроінтеграційних зобов'язань.

Відставання правового регулювання від темпів технологічного розвитку вказує на слабку пристосованість діючої нормативної основи до інтенсивних цифрових змін. Введення гнучких правових механізмів та систематичне оновлення законодавства в секторах штучного інтелекту, хмарних технологій й розгляду значних обсягів інформації буде сприяти зростанню його актуальності. В той же час брак фахових експертів та складність передбачення тенденцій технологічного характеру формують значні перепони для результативного нормотворення.

Проблема обмеженої регламентації публічно-приватного партнерства виражає недостатність участі приватного сектору в гарантуванні кібербезпеки, незважаючи на його головне значення у функціонуванні критичної інфраструктури. Напрацювання спеціальних правових норм та системи заохочень здатне інтенсифікувати таке співробітництво, проте недовіра бізнесу до інституцій держави і ризик витоку чутливих даних продовжують залишатися вагомими факторами стримувального характеру.

Недостатня деталізація процедур реагування на кіберінциденти свідчить про брак єдиного правового порядку дій в кризових обставинах. Уніфікація процесів і фіксація стандартів кризового управління спроможні збільшити оперативність та скоординованість реагування. Однак бюрократична інерція і брак узгоджених технічних стандартів здатні мінімізувати прикладну результативність таких заходів.

Неврегульованість питань кібербезпеки на регіональному та місцевому рівнях вказує на надмірну централізацію системи публічного управління в згаданому секторі. Напрацювання типових положень для органів місцевого самоврядування і передача певних повноважень дасть змогу збільшити спроможність територіальних громад. В той же час обмежений фінансовий потенціал і недостатній ступінь цифрової компетентності службовців значно ускладнюють втілення зазначених ініціатив.

Врешті-решт, обмеженість правових інструментів забезпечення кібербезпеки на тлі воєнного стану робить актуальною необхідність щодо спеціального правового порядку управління. Збільшення повноважень кризових центрів та зростання координації вважаються аргументованими на тлі агресії збройного харатктеру, проте вони супроводжуються ризиками порушення балансу між вимогами національної безпеки й додержанням прав та свобод людини і, крім того, загрозою перебільшеної централізації управлінських рішень.

Відтак, вдосконалення нормативно-правового забезпечення публічного управління кібербезпекою України вимагає не тільки оновлення законодавства, а також грунттовної інституційної трансформації, зростання міжсекторальної взаємодії і зважання на специфіку воєнного та післявоєнного становлення держави.

Що стосується удосконалення організаційного механізму, то пропозиції щодо усунення проблем організаційного забезпечення публічного управління у сфері кібербезпеки України наведено у табл. 3.3.

Таблиця 3.3

Пропозиції щодо усунення проблем організаційного забезпечення публічного управління у сфері кібербезпеки України

№	Проблема	Пропозиції щодо усунення	Відповідальні органи публічної влади	Можливі перешкоди
1	Нечітка структура і розподіл повноважень	Оптимізувати організаційну структуру системи кібербезпеки; чітко	Верховна Рада України, Рада національної безпеки і оборони	Наявність інституційної інерції; опору органів влади до

		закріпити функції і зони відповідальності суб'єктів публічного управління	України, Кабінет Міністрів України	змін в організаційній структурі
2	Фрагментарність координації між суб'єктами кібербезпеки	Створити єдину централізовану систему координації; уніфікувати процедури міжвідомчої взаємодії	Рада національної безпеки і оборони України, Кабінет Міністрів України, Державна служба спеціального зв'язку та захисту інформації	Відсутність єдиних організаційних стандартів; наявність перешкод для інтеграції різних інституцій в єдину систему
3	Недостатнє кадрове забезпечення та дефіцит фахівців	Удосконалити систему підготовки та перепідготовки кадрів; сформувати механізми мотивації й утримання висококваліфікованих фахівців	Кабінет Міністрів України, Мінцифри, Міносвіти, органи сектору безпеки і оборони	Наявність конкуренції з приватним сектором; обмеженість фінансових ресурсів
4	Обмежені ресурси та технологічна відсталість	нарощувати ресурсний потенціал забезпечення кіберпідрозділів	Кабінет Міністрів України, Мінфін, Мінцифри, Рада національної безпеки і оборони України	Наявність бюджетних обмежень та значної залежності від міжнародної технічної допомоги
5	Недостатня інтеграція стратегічного планування та управлінських процедур	Запровадити єдину систему стратегічного та оперативного планування у сфері кібербезпеки; інституціоналізувати ризик-орієнтований підхід	Рада національної безпеки і оборони України, Кабінет Міністрів України	Наявність формалізму у плануванні; низького рівня управлінської культури
6	Недостатня регіональна представленість та взаємодія з місцевим рівнем	Сформувати регіональні координаційні механізми кібербезпеки; інтегрувати органи місцевого самоврядування до загальнодержавної системи реагування на кіберінциденти	Кабінет Міністрів України, Мінрегіон, органи місцевого самоврядування	Наявність нерівномірності у розвитку регіонів; дефіциту кваліфікованих кадрів на місцях
7	Слабка міжвідомча та міжнародна взаємодія	Посилити міжвідомчий обмін інформацією; посилити міжнародне співробітництво у сфері кібербезпеки	Рада національної безпеки і оборони України, Міністерство закордонних	Наявність правових обмежень обміну даними; ризиків витоку

			справ України, Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації	конфіденційної інформації

Джерело: власна розробка автора

Проблема нечіткої організаційної структури та розподілу повноважень вказує на інституційне незбалансування системи кібербезпеки. Рекомендовані заходи стосовно оптимізації структури й чіткого затвердження функцій та зон відповідальності передбачають зростання керованості системи і мінімізацію терміну ухвалення управлінських рішень. В той же час інституційна інерція і опір змінам зі сторони певних органів влади здатні суттєво пригальмувати процес реформування.

Фрагментарність координації між суб’єктами кібербезпеки продовжує залишатися одним з головних факторів зменшення результативності публічного управління. Формування єдиної централізованої системи координації, а також уніфікація процесів міжвідомчої взаємодії призначені для ліквідації дублювання функцій та збільшення узгодженості дій в кризових випадках. У той же час неіснування стійких організаційних стандартів та складність введення різних інституцій в єдину систему створюють додаткові перепони організаційного плану.

Недостатнє кадрове забезпечення та дефіцит висококваліфікованих фахівців обмежують здатність держави до системної протидії кіберзагрозам. Покращення системи підготовки та перепідготовки персоналу і, крім того, створення дієвих механізмів мотивації й утримання фахівців вважаються стратегічно значущими заходами. Однак конкуренція з приватною сферою та фінансова обмеженість державного бюджету значно мінімізують змоги їхнього практичного втілення.

Обмежені ресурси органів публічного управління мають негативний вплив на спроможність вчасно встановлювати і знешкоджуват кіберзагрози. Збільшення ресурсного потенціалу кіберпідрозділів націлені на зростання

загального ступеня кіберстійкості держави. В той же час існуючі наявні бюджетні обмеження й велика залежність від міжнародного технічного сприяння формують ризики нестійкості подібного розвитку.

Недостатня інтеграція стратегічного планування та управлінських процедур свідчить про незначне узгодження між довгостроковими цілями й оперативними управлінськими рішеннями в секторі кібербезпеки. Введення єдиної системи стратегічного та оперативного планування, а також інституціоналізація ризик-орієнтованого підходу повинні допомогти збільшити передбачуваність й результативність управління. Проте формалізм в плануванні і слабкий ступінь управлінської культури здатні звести нанавець передбачуваний результат від подібних змін.

Недостатня регіональна представленість і слабка взаємодія з місцевим рівнем спричиняють нерівномірність кіберстійкості на території країни. Створення регіональних координаційних механізмів, а також включення органів місцевого самоврядування в загальнодержавну систему реагування на кіберінциденти дадуть змогу зміцнити вертикаль управління. В той же час нерівномірність соціально-економічного зростання регіонів та брак кваліфікованого персоналу на місцях продовжують залишатися значними стримувальними факторами.

Слабка міжвідомча та міжнародна взаємодія обмежує змоги України стосовно швидкого обміну даними й спільного реагування на транснаціональні кіберзагрози. Зростання міжвідомчого обміну інформацією й зростання міжнародної співпраці в секторі кібербезпеки – необхідна передумова зростання результативності публічного управління. В той же час обмеження доступу до даних й ризик витоку конфіденційної інформації заслуговують на особливу увагу у процесі становлення подібних механізмів.

Підсумовуючи, розгляд рекомендованих заходів вказує на те, що удосконалення організаційного забезпечення публічного управління у сфері кібербезпеки України вимагає комплексного підходу, що сполучає інституційні реформи, зростання кадрових ресурсів, технологічне оновлення

й зростання міжрівневої та міжнародної координації, зважаючи на існуючі внутрішні та зовнішні обмеження.

Що стосується інформаційно-технічного механізму, то пропозиції щодо усунення проблем інформаційно-технічного забезпечення публічного управління у сфері забезпечення кібербезпеки України наведено у табл. 3.4

Таблиця 3.4

Пропозиції щодо усунення проблем інформаційно-технічного забезпечення публічного управління у сфері забезпечення кібербезпеки України

№	Проблема	Пропозиції щодо усунення	Відповідальні органи публічної влади	Можливі перешкоди
1	Зношеність та фрагментарність інформаційно-технічної інфраструктури	Модернізувати інформаційно-технічну інфраструктуру органів публічної влади; оновити програмно-апаратні комплекси	Кабінет Міністрів України, Мінцифри, Мінфін, Рада національної безпеки і оборони України	Наявність бюджетних обмежень; тривалі процеси оновлення; залежність від зовнішніх постачальників
2	Відсутність єдиних технічних стандартів і протоколів взаємодії	Розробити та впровадити єдині технічні стандарти і протоколи інформаційної взаємодії; уніфікувати програмно-апаратні рішення	Мінцифри, Державна служба спеціального зв'язку та захисту інформації, Кабінет Міністрів України	Наявність технічної несумісності існуючих систем та опору відомств під час стандартизації
3	Недостатній рівень автоматизації процесів управління кібербезпекою	Запровадити автоматизовані системи збору, аналізу та обробки даних про кіберінциденти; цифровізувати управлінські процеси	Мінцифри, Державна служба спеціального зв'язку та захисту інформації, Рада національної безпеки і оборони України	Наявність високої вартості технологічних рішень та дефіциту у кваліфікованих технічних кадрах
4	Обмежені можливості моніторингу та прогнозування кіберзагроз	Удосконалити інформаційно-аналітичні системи моніторингу кіберзагроз; впровадити технології аналізу	Державна служба спеціального зв'язку та захисту інформації, Служба безпеки України, Мінцифри, Рада	Наявність технологічної складності; обмеженого доступу до даних; фінансових обмежень

		великих даних і кореляції подій	національної безпеки і оборони України	
5	Недостатній рівень захисту державних інформаційних ресурсів	Посилити криптографічний та технічний захист інформації; удосокналити систему резервного копіювання та відновлення даних	Державна служба спеціального зв'язку та захисту інформації, Кабінет Міністрів України, Мінцифри	Наявність високої вартості засобів захисту; фрагментарності їх впровадження
6	Проблеми інтеграції хмарних технологій та нових цифрових рішень	Удосконалити технічні механізми використання хмарних сервісів; розробити вимоги до безпечної інтеграції цифрових рішень	Мінцифри, Державна служба спеціального зв'язку та захисту інформації, Кабінет Міністрів України	Наявність підвищеної небезпеки кіберризиків; відсутності єдиних технічних підходів
7	Слабка інтеграція інформаційно-технічного забезпечення з управлінськими процесами	Інтегрувати інформаційно-аналітичні системи до процесів стратегічного та оперативного управління кібербезпекою	Рада національної безпеки і оборони України, Кабінет Міністрів України, Мінцифри	Наявність низького рівня управлінської цифрової культури та формалізму у використанні цифрових рішень

Джерело: власна розробка автора

Зношеність та фрагментарність інформаційно-технічної інфраструктури вказує на критичну необхідність у її модернізації, а також оновленні. Рекомендована модернізація програмно-апаратних комплексів органів публічної влади повинна створити відповідні умови для зростання ступеня захищеності інформаційних систем та їхньої сумісності із новітніми інструментами кіберзахисту. В той же час бюджетні обмеження, тривалість оновлення інфраструктури й залежність від постачальників технологій ззовні обумовлюють великі ризики для здійснення згаданих заходів у короткі терміни.

Відсутність єдиних технічних стандартів і протоколів взаємодії спричиняє слабкий ступінь узгодженості інформаційних систем різних органів влади. Напрацювання і введення уніфікованих стандартів інформаційної взаємодії призначене гарантувати централізоване відстеження кіберзагроз та збільшити результативність координування реагування. Водночас технічна

несумісність уже існуючих систем, а також спротив певних установ щодо процедур стандартизації здатні суттєво ускладнити здобуття єдиного технічного простору.

Недостатній рівень автоматизації процесів управління кібербезпекою здійснює негативний вплив на швидкість ухвалення управлінських рішень. Введення автоматизованих систем збирання, вивчення й опрацювання інформації щодо кіберінцедентів буде сприяти зменшенню тривалості реагування і покращенню якості управлінських рішень. Проте велика вартість новітніх технологічних рішень та брак кваліфікованого технічного персоналу продовжують залишатися значними стримувальними факторами цифрової трансформації.

Обмежені можливості моніторингу та прогнозування кіберзагроз свідчать про недостатнє становлення інформаційно-аналітичних спроможностей держави. Зростання систем моніторингу, введення технологій розгляду значних обсягів інформації та співвідношення подій в реальному часі повинні збільшити ступінь проактивності публічного управління в секторі кібербезпеки. В той же час технологічна складність подібних рішень, обмежена доступність до релевантної інформації та фінансові обмеження ослаблюють динаміку їх введення.

Недостатній рівень захисту державних інформаційних ресурсів – результат фрагментарного введення криптографічних і технічних засобів захисту і, крім того, нерозвиненого характеру систем резервного копіювання й відновлення інформації. Зростання технічного й криптографічного захисту повинне мінімізувати ризики втрачання чи компроментації даних, однак велика вартість подібних інструментів та нерівномірне їхнє використання у різних органах влади значно обмежують результативність зазначених заходів.

Проблеми інтеграції хмарних технологій та нових цифрових рішень вказують на нестачу врегулювання технічних механізмів їх застосування в органах публічного управління. Підвищення вимог щодо безпечного впровадження хмарних сервісів призначене зменшити ступінь додаткових

кіберризиків, проте неіснування єдиних технічних підходів та підвищена вразливість подібних рішень вимагають збільшеного контролювання й стандартизації.

Слабка інтеграція інформаційно-технічного забезпечення з управлінськими процесами вказує на обмежене застосування можливостей інформаційних систем для сприяння стратегічному й оперативному управлінню кібербезпекою. Введення інформаційно-аналітичних систем в процедури ухвалення рішень повинне допомогти зростанню аргументованості і вчасності управлінських дій. В той же час слабкий ступінь управлінської цифрової культури й формалізм в застосуванні ІТ-рішень погіршують результативність такого введення.

Підсумовуючи, розгляд таблиці свідчить, що вдосконалення інформаційно-технічного забезпечення публічного управління у сфері кібербезпеки України вимагає комплексного підходу, що сполучає технологічну модернізацію, стандартизацію технічних рішень, зростання аналітичних здатностей і грунтовне введення ІТ-інструментів у систему управління, зважаючи на існуючі ресурсні та організаційна обмеження.

Очікувані результати реалізації комплексного механізму удосконалення публічного управління у сфері забезпечення кібербезпеки України доречно формулювати, зважаючи на його стратегічну ціль, завдання та принципи й, крім того, новітні безпекові виклики:

1. Формування цілісної та узгодженої системи публічного управління кібербезпекою. Гарантування системності нормативно-правових, організаційних, а також інформаційно-технічних елементів управління, що мінімізує фрагментарність рішень та покращить координацію дій суб’єктів публічної влади.

2. Підвищення ефективності координації та міжвідомчої взаємодії. Чіткий поділ повноважень та введення ефективних координаційних механізмів будуть сприяти швидкому ухваленню управлінських рішень і зменшенню дублювання функцій у процесі реагування на кіберінциденти.

3. Зміцнення кіберстійкості держави та критичної інформаційної інфраструктури. Зростання здатності державних інформаційних систем протистояти кібератакам, гарантувати постійність діяльності й оперативне відновлення на тлі криз та воєнного стану.

4. Підвищення рівня правової визначеності та адаптивності регулювання. Удосконалення законодавства в секторі кібербезпеки гарантуватиме його адекватність новітнім технологічним трендам та міжнародним стандартам і, крім того, збільшить прогнозованість управлінських рішень.

5. Посилення інформаційно-технічних та аналітичних спроможностей. Зростання автоматизованих систем моніторингу, розгляду та передбачення кіберзагроз гарантуватиме перехід до проактивної моделі управління кіберризиками.

6. Активізація публічно-приватного та міжнародного співробітництва. Участь приватного сектору й міжнародних партнерів у створенні належних умов для кібербезпеки буде сприяти зростанню ресурсної здатності держави, а також інтеграції України в міжнародне кібербезпекове середовище.

7. Підвищення готовності до реагування на гібридні та воєнні кіберзагрози. Введення особливого управлінського порядку та кризових механізмів дасть можливість результативніше функціонувати системі публічного управління в обставинах воєнного стану.

Підсумовуючи усе вищесказане, можемо зробити висновок, що на фоні цифровізації суспільства, гібридної війни і збільшення обсягів та складності кіберзагроз кібербезпека отримує статус одного із основних складових національної безпеки держави. Результативність її гарантування перебуває в прямій залежності від здатності системи публічного управління вчасно пристосовуватися до інтенсивних технологічних та безпекових змін. Обґрунтовано, що удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки повинне відбуватися комплексно й включати синхронний розвиток нормативно-правового, організаційного, та

інформаційно-технічного компонентів. Головними векторами подібного вдосконалення встановлено узгодження законодавства із міжнародними й європейськими стандартами, інституціоналізацію дієвих координаційних механізмів, введення ризик-орієнтованого й проактивного підходів до управління кібербезпекою, зростання систем стратегічного й оперативного планування і, крім того, збільшення значення аналітичних та цифрових засобів під час ухвалення управлінських рішень. Доказано, що значуща умова зростання ефективності публічного управління у сфері кібербезпеки – вироблення новітньої управлінської культури й активізація міжвідомчої, міжрівневої та міжнародної співдії, в тому числі у межах публічно-приватного партнерства. Особливу роль відіграє введення органів місцевого самоврядування у загальнодержавну систему забезпечення кібербезпеки для того, щоб покращити регіональну кіберстійкість.

Втілення рекомендованих шляхів удосконалення механізмів публічного управління буде сприяти утворенню цілісної, адаптивної і стійкої системи забезпечення кібербезпеки України, яка спроможна результативно протистояти нинішнім та майбутнім кіберзагрозам, що, своєю чергою, сформує відповідне підгрунтя для захисту національних інтересів, постійної діяльності органів публічної влади і зростання довіри суспільства до державної політики в секторі цифрової безпеки.

3.3. Розвиток інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури

В обставинах цифровізації суспільних процесів і збільшення залежності держави й економіки від сталої діяльності інформаційно-комунікаційних систем питання кіберзахисту об’єктів критичної інфраструктури стає особливо актуальним. Критична інфраструктура включає комплекс об’єктів та систем, порушення функціонування котрих здатне зумовити великі соціально-економічні ефекти, загрози національній безпеці, а також життєдіяльності

громадян. В зазначених обставинах кіберпростір стає одним з основних фронтів протиборства, де кібератаки все більш часто застосовуються як засіб дестабілізації державних структур та стратегічно значущих сфер.

Новітні виклики, в тому числі збільшення складності та масштабів кіберзагроз, спричиняють потребу переходу від усталених інструментів інформаційної безпеки до інноваційних інструментів кіберзахисту. Мовиться про введення технологій штучного інтелекту, машинного навчання, автоматизованих систем встановлення загроз, хмарних і розподілених рішень, і, крім того, про зростання проактивних моделей управління кіберризиками. Інноваційний розвиток у сфері кіберзахисту набуває значення визначального фактора зростання стійкості об’єктів критичної інфраструктури до кібератак і гарантування постійності їх діяльності.

Особливе значення ця проблематика відіграє для України на тлі гібридної війни, під час якої кібератаки націлені не тільки на те, щоб порушити інформаційні системи, а також щоб підірвати довіру до держави і її інституцій. Це спричиняє необхідність щодо системного наукового розуміння інноваційних підходів до кіберзахисту і створення дієвих механізмів впровадження сучасних інструментів безпеки на об’єктах критичної інфраструктури.

Об’єкти критичної інфраструктури – це об’єкти інфраструктури, системи, їхні складові, а також їхній комплекс, котрі вважають значущими для економіки, національної безпеки й оборони, порушення роботи котрих здатне зашкодити життєво важливим національним інтересам.

Відповідно до законодавства, «віднесення об’єктів до критичної інфраструктури здійснюється за сукупністю критеріїв, що визначають їх соціальну, політичну, економічну, екологічну значущість для забезпечення оборони країни, безпеки громадян, суспільства, держави і правопорядку, зокрема для реалізації життєво важливих функцій та надання життєво важливих послуг» [125]. При цьому, «кіберзахист об’єкта критичної інфраструктури забезпечується шляхом впровадження на об’єкті критичної

інформаційної інфраструктури комплексної системи захисту інформації або системи інформаційної безпеки з підтвердженою відповідністю» [116]. Кіберзахист об'єкта критичної інфраструктури є «складовою частиною робіт із створення та експлуатації об'єкта критичної інформаційної інфраструктури. Заходи з кіберзахисту передбачаються та впроваджуються на всіх стадіях життєвого циклу об'єкта критичної інформаційної інфраструктури» [116]. З огляду на важливість кібербезпеки в нинішніх реаліях об'єкти критичної інфраструктури стають особливою ціллю для кіберзлочинців і кіберзагроз. Згадані об'єкти мають у своєму складі енергетичні системи, транспорт, комунікаційні мережі, медичні заклади й інші значущі галузі, котрі гарантують потребу функціонування соціуму.

Напади на критичну інфраструктуру здатні обумовлювати значні наслідки, в тому числі спричинити перерви в наданні послуг, втрату конфіденційності інформації чи навіть становити загрозу для життя громадян. Зважаючи на безперервний розвиток технологій і збільшення обсягу кіберзагроз, захист критичної інфраструктури являється вкрай вагомим завданням.

Варто зауважити, що «потреба постійно захищати критичну інфраструктуру від усіх видів фізичних загроз і небезпек, в тому числі кіберзагроз, обумовлює необхідність побудови системи управління критичною інфраструктурою, спрямованої на забезпечення її захисту, безпеки та стійкості з залученням до відповідних зусиль і заходів усього суспільства: від окремих громадян, місцевих громад, суб'єктів господарювання до органів державної влади» [97]. Наразі держава активно курирує питання інтеграції інноваційних інтегрованих технологій, щоб забезпечити об'єкти критичної інфраструктури в обставинах кібервійни.

Варто зазначити, що «набутий Україною досвід у протистоянні безпрецедентним за масштабом та інтенсивністю атакам на критичну інфраструктуру в умовах повномасштабної війни є унікальним і має виняткове значення як для вдосконалення національної системи захисту, так і для

оновлення міжнародних стандартів та підходів у цій сфері. Жодна країна у новітній історії не стикалася з настільки систематичним і цілеспрямованим використанням військових та кібернетичних засобів для руйнування основ життєзабезпечення суспільства» [22]. Зауважимо, що «такий гіркий досвід дозволив винести низку ключових уроків. Насамперед, атаки на великі енергетичні об'єкти виявили критичну вразливість централізованих систем, що зумовило нагальну необхідність підвищення стійкості через децентралізацію, шляхом розвитку розподіленої генерації (включаючи мобільні газотурбінні станції, когенераційні установки, відновлювані джерела енергії), створення мікромереж та резервних джерел живлення для забезпечення автономності об'єктів критичної інфраструктури та населених пунктів» [22]. Крім децентралізації генерації, значущим вважається, до того ж, аспект гарантування фізичного захисту головних об’єктів від безпосередніх кінетичних атак, що містить як інженерне укріплення об'єктів, так і розбудову ешелонованої системи протиповітряної і протиракетної оборони.

До того ж, «удари по транспортній інфраструктурі підкреслили потребу в диверсифікації та розвитку альтернативних логістичних маршрутів для забезпечення безперебійного та безпечного постачання необхідних ресурсів для підтримки економіки, оборони та гуманітарних потреб» [13]. Критично значущою виявилася спроможність швидко ремонтувати й відновлювати діяльність пошкоджених об'єктів критичної інфраструктури, що, своєю чергою, постійно ставить вимогу формування матеріально-технічних резервів, підготовки ремонтних бригад і напрацювання конкретних планів дій.

Загалом, всі загрози спричиняють необхідність розробки єдиної державної політики в секторі гарантування кібербезпеки на об’єктах критичної інфраструктури, втілення котрої визначає законодавчі, організаційні, технічні, освітні й решту заходів. Здійснимо більш детальний розгляд згаданих заходів.

З-поміж технічних заходів виокремлюються: 1) створення системи встановлення і здійснення превентивних заходів щодо загроз (IDS/IPS); 2)

сегментація мережі; 3) постійна модернізація програмного забезпечення й операційних систем; 4) шифрування інформації; 5) аутентифікація, а також управління доступом; 6) резервне копіювання і відновлення; 7) систематичне формування резервних копій критичної інформації та планів відновлення.

Організаційні заходи встановлюють: 1) існування відповідних процесів щодо кібербезпеки; 2) інцидент-менеджмент, формування і сприяння процедурам для встановлення, реагування й ліквідації наслідків кіберінцидентів; 3) постійний аудит і тестування; 4) співдія приватної сфери із державними органами в секторі кібербезпеки.

Не менш значущими вважаються освітні, правові та превентивні заходи, суть котрих орієнтована на: 1) навчання і зростання компетенції працівників; 2) зменшення ризиків, що мають зв’язок із атаками соціальної інженерії; 3) контролювання й моніторинг поточного стану в кіберпросторі; 4) додержання законодавства в секторі кібербезпеки.

Як зазначає Л. Арсенович, система публічної політики у сфері захисту критичної інфраструктури націлена на утворення сукупності ресурсних, організаційних, методологічних, інженерно-технічних, нормативно-правових, а також інформаційно-аналітичних заходів, орієнтованих на:

– «визначення суб’єктів національної системи захисту критичної інфраструктури та законодавчих вимог до принципів, стратегічних завдань, пріоритетів та підходів щодо захисту критичної інфраструктури;

– створення умов спрямованих на ефективне зниження і контроль за ризиками безпеки та швидке відновлення надання життєво важливих функцій та послуг у разі реалізації загроз і порушення функціонування критичної інфраструктури;

– запровадження державно-приватного партнерства, а також взаємодію суб’єктів господарювання та населення з питань забезпечення захисту та стійкості критичної інфраструктури;

– створення системи раннього виявлення загроз критичній інфраструктурі, а також на забезпечення міжнародного співробітництва у сфері захисту критичної інфраструктури;

– визнання необхідності забезпечення безпеки та стійкості критичної інфраструктури» [6].

Разом з тим, система публічної політики у сфері захисту критичної інфраструктури скеровує свій вектор на те, щоб запобігти проявам несанкціонованого втручання у безпеку об'єктів критичної інфраструктури через:

– «розроблення нормативно-правової бази з питань забезпечення безпеки об'єктів критичної інфраструктури, державних цільових програм із захисту критичної інфраструктури, заходів з контролю за ризиками безпеки, виявлення, запобігання та ліквідації наслідків інцидентів безпеки на об'єктах критичної інфраструктури, а також методології аналізу результативності державної політики у сфері захисту критичної інфраструктури;

– встановлення вимог із забезпечення безпеки об'єктів критичної інфраструктури, а також проведення аналізу викликів та загроз, що впливають на стійкість критичної інфраструктури;

– підготовки, перепідготовки, підвищення кваліфікації та тренування працівників національної системи захисту критичної інфраструктури;

– запобігання проявам несанкціонованого втручання в її функціонування, а також шляхом попередження кризових ситуацій, що порушують безпеку критичної інфраструктури;

– забезпечення взаємодії національної системи захисту критичної інфраструктури з європейськими та євроатлантичними системами» [6].

Наразі нинішні науковці досліджують концепцію захисту критичної інфраструктури у системі національної безпеки України як варіанти двох моделей, зокрема:

– «модель добровільного підходу, яка передбачає політико-лібералізаційне управління, добровільне дотримання стандартів,

саморегулювання, а також самостійне формування та реалізацію політики захисту критичної інфраструктури;

– модель відповідальності, яка передбачає обов'язкове дотримання нормативно-правових актів, а також заходи впливу на операторів об'єктів критичної інфраструктури за порушення у сфері безпеки» [6].

Кіберзахист весь час розвивається, зважаючи на безперервне збільшення обсягу й складності кіберзагроз. З метою зростання захисту об'єктів критичної інфраструктури потрібно вивчити ряд новітніх технологічних тенденцій в кіберзахисті, а саме:

– «штучний інтелект та машинне навчання: штучний інтелект та машинне навчання використовуються для аналізу величезних обсягів даних, що допомагає виявляти аномалії та прогнозувати потенційні загрози. Алгоритми навчаються розпізнавати відхилення від звичайної поведінки мережі та реагувати на них» [12];

– «аналіз біг даних та розпізнавання загроз: використання технологій аналізу великих обсягів даних допомагає в ідентифікації та розпізнаванні підозрілих патернів у мережі, що можуть свідчити про потенційні загрози» [63];

– «блокчейн та криптографія: застосування технологій блокчейну та криптографії допомагає у створенні безпечних та непідробних систем збереження даних, а також у впровадженні безпечних методів ідентифікації та автентифікації» [111];

– «Інтернет речей (IoT) та захист вбудованих систем: об'єкти критичної інфраструктури можуть використовувати безліч підключених до Інтернету пристроїв. Це потребує розробки та впровадження надійних методів захисту вбудованих систем, щоб запобігти можливим кібератакам через ці пристрої» [51];

– «аналітика загроз та виявлення атак: використання спеціалізованих платформ для аналізу загроз дозволяє відстежувати, реагувати та виявляти атаки в реальному часі» [55];

– «автоматизовані засоби захисту: розвиток автоматизованих засобів захисту, які виявляють, аналізують та реагують на загрози без значного втручання людини, дозволяє забезпечити швидкий реакційний час та мінімізувати вплив кібератаки» [55];

– «захист на рівні обробки даних: розвиток методів шифрування, механізмів захисту від утечок даних та контролю доступу до інформації на рівні обробки даних сприяє підвищенню загального рівня кіберзахисту» [55].

Розгляд і введення згаданих технологічних тенденцій в галузі критичної інфраструктури дає можливість реагувати на складність новітніх кіберзагроз і гарантує зростання захищеності систем в режимі реального часу.

На думку А. Давидюк, «захист даних у сфері критичної інфраструктури стає дедалі важливішим, оскільки технології стають більш складними та загрози кібербезпеки зростають. Один з найважливіших методів захисту цих даних – шифрування» [33]. Шифрування та захист даних – це «важливі складові кіберзахисту критичної інфраструктури, які сприяють у запобіганні витоку конфіденційної інформації та збереженні цілісності даних в умовах зростаючих кіберзагроз» [33]. Шифрування даних – це процедура трансформації даних в незрозумілий вигляд (шифр) для того, щоб зберегти конфіденційність і цілісність інформації. В аспекті критичної інфраструктури це значить використання шифрування з метою захисту інформації, передача котрої відбувається по мережі і яка зберігається на серверах й інших приладах.

Застосування шифрування даних в транспортних мережах, як-от використання протоколів HTTPS для веб-трафіку, і застосування шифрування інформації на рівні файлів, папок і дисків сприяють в гарантуванні безпеки від зловмисних атак, включно з перехопленням інформації.

Шифрування додатково можна застосовувати з метою захисту інформації від несанкціонованого доступу. Шифрування даних на підставному рівні значуще, тому що воно забезпечує додатковий захисний бар’єр навіть в разі, коли зловмиснику вдасться одержати фізичний доступ до устаткування або файлів.

Крім того, шифрування передбачає використання шифрувальних алгоритмів і ключів, щоб гарантувати доступ лише авторизованим користувачам. Застосування потужних алгоритмів шифрування і безпечних ключів – значущі складові для попередження розшифрування даних злочинцями.

Використання шифрування і захист інформації значущі не тільки для веб-переглядачів, а також для усіх приладів і систем в критичній інфраструктурі, які здійснюють опрацювання конфіденційних даних. Це охоплює сервери, мережеве устаткування, сховища інформації, мобільні прилади й велику кількість іншого.

Як зазначає С. Кузьмірук, «постійне вдосконалення технологій та взаємодія всіх сторін можуть забезпечити ефективний та стійкий кіберзахист об’єктів критичної інфраструктури в умовах сучасної кіберзагрози. Важливе значення набувають інноваційні аспекти впровадження інтегрованих систем кібербезпеки об’єктів критичної інфраструктури на базі штучного інтелекту. Сучасний генеративний штучний інтелект або інтелектуальний штучний інтелект забезпечує багато переваг у сфері кібербезпеки – від автоматизації завдань і зменшення помилок персоналу до використання прогнозової аналітики для підтримки виявлення загроз» [64].

Штучний інтелект необхідний для автоматизації оперативного реагування на інциденти безпеки. Зокрема, «прогнозуючий штучний інтелект може оптимізувати механізм виявлення загроз і створювати ефективні рішення з кібербезпеки, узгоджені з ландшафтом загроз, які постійно змінюється. Ці системи штучного інтелекту, по-перше, самоконтролюються та самонавчаються, а, по-друге, можуть застосовувати аналіз у непередбачуваних ситуаціях і приймати рішення на основі власних спостережень. Інтеграція інтелектуальних систем дозволяє автоматизувати виявлення кіберзагроз, а використання алгоритмів машинного навчання підвищує ефективність комплексних заходів з протидії кібератакам» [64]. Штучний інтелект «відіграє ключову роль у зниженні ризиків кіберзагроз об’єктів критичної

інфраструктури завдяки можливостям виявлення аномалій, автоматизації реакцій на інциденти, прогнозування та запобігання кіберзагрозам, покращення аутентифікації користувачів, оптимізації управлінням вразливостями, розпізнавання фішингових кібератак та підтримки у розслідуванні кіберінцидентів. Аналізуючи великі обсяги даних у реальному часі, штучний інтелект забезпечує швидке виявлення та блокування загроз, що підвищує ефективність захисту своїх систем та мінімізує шкоду від кібератак» [170]. Надійна кібербезпека особливо значущою стала в нинішню цифрову еру в обставинах, які весь час зазнають змін. Як і у великому числі інших галузей, у майбутньому значення штучного інтелекту у кібербезпеці відіграватиме ще більш вагому роль.

Введення штучного інтелекту – потрібний еволюційний крок для гарантування різнопланового, дієвого кіберзахисту, враховуючи економічну доречність. Його використання дасть можливість істотно поліпшити стан гарантування кібербезпеки, посилити захищеність інформаційних ресурсів, а також інформаційно-комунікаційних систем об’єктів критичної інфраструктури держави задля оперативного реагування на наявні кіберзагрози, заздалегідь здійснити їх нейтралізацію.

В аспекті введення інтегрованих систем кіберзахисту значущою вважається координація між державою, представниками приватного сектору і міжнародними контрагентами щодо питань протидії новітнім кіберзагрозам. Варто зазначити, що введення інтегрованих систем кіберзахисту інформації й кібербезпеки об’єктів критичної інфраструктури реалізується, враховуючи:

1) «комплексного підходу до захисту об’єктів критичної інфраструктури;

2) централізованого управління кібербезпекою;

3) постійного підвищення фахового рівня персоналу таких об’єктів» [64].

Подібний підхід ставить вимогу щодо використання штучного інтелекту з метою: встановлення і реагування на кіберзагрози в режимі реального часу;

автоматизації заходів кіберзахисту, фахової підготовки працівників, системного захисту інформації; оперативної відбудови після кібератак і, крім того, з метою підтримки співробітництва з міжнародними партнерами в зазначеному секторі. В аспекті згаданого штучний інтелект здатний здійснювати аналіз аномальної поведінки працівників, автоматично відповідати на інциденти, оновлювати програмне забезпечення, шифрувати інформацію, проводити моніторинг даних, давати оцінку наслідків кібератак і здійснювати координацію дій певних структур.

Відтак, застосування штучного інтелекту – це перспективний інноваційний вектор в секторі інформаційної безпеки, що обумовлює введення інтегрованих інформаційно-аналітичних систем, основуючись на штучному інтелекті з метою збільшення результативності кіберзахисту, оперативного реагування і протидії кібератакам на об’єкти критичної інфраструктури країни.

Аудит є «одним з ключових процесів у забезпеченні ефективності та стійкості критичної інфраструктури перед кіберзагрозами» [95]. Аудит охоплює грунтовний огляд систем, мереж і механізмів з метою виявлення потенційних слабких місць і вразливості, що сприяє встановленню ймовірних ризиків і гарантувати прозорість стану кібербезпеки. Безперервне покращення зводиться до покращення заходів безпеки, базуючись на результатах аудиту й сучасних підходах до кіберзахисту, що передбачає покращення процесів, модернізацію технологій і введення нових стратегій для того, щоб запобігти потенційним загрозам.

Основна частина аудиту – оцінювання поточних систем безпеки і їх відповідності стандартам безпеки і, крім того, напрацювання планів для того, щоб виправити встановлені недоліки і вразливості. Значуща частина згаданого процесу, крім того, – встановлення основних показників ефективності, котрі дають змогу оцінити результативність заходів кіберзахисту й дієвість планів покращення.

Блокчейн-технологія, що складає основу криптовалют, показує великий потенціал в секторі кібербезпеки, в тому числі щодо гарантування безпеки інформації критичної інфраструктури. З огляду на своє дистрибутивне походження, блокчейн гарантує збереження даних у незмінній формі, завдяки чому вона стає стійкою до підробок та змін несанкціонованого характеру.

Застосування блокчейн-технології на об’єктах критичної інфраструктури здатне сприяти у розв’язанні проблеми безпеки інформації, гарантуючи автентифікацію транзакцій і обмежуючи доступ до конфіденційних даних. Приміром, в енергетичних системах блокчейн можна застосовувати, щоб вести облік споживання енергії і, крім того, щоб управляти дистрибуцією електроенергії між різними споживачами, гарантуючи прозорість та захист від шахрайства. Крім того, «блокчейн може використовуватися для забезпечення безпеки IoT-пристроїв, адже його дистрибутивна структура дозволяє знизити ризик централізованих атак. Завдяки інтеграції технології блокчейн у мережі IoT, дані можуть зберігатися на розподілених вузлах, що ускладнює доступ до них зловмисників і підвищує загальний рівень безпеки» [4].

Квантова криптографія гарантує захист інформації в реальному часі, що вважається критично значущим для систем, які керують критичною інфраструктурою. Це дає змогу безпечним чином здійснювати передачу даних між частинами інфраструктури, приміром, між електростанціями й мережами управління. У випадку намагання перехоплення чи зміни квантових сигналів система в автоматичному режимі помічає вторгнення, що дає можливість негайно здійснити заходи, щоб захистити інформацію. Крім того, «квантові комп'ютери, хоч і ще не стали масовими, обіцяють змінити ландшафт шифрування. Вони здатні виконувати обчислення, які є непосильними для класичних комп'ютерів, включаючи злому традиційних методів шифрування. Тому розробка нових квантових алгоритмів для шифрування даних є нагальною потребою для забезпечення довгострокової безпеки критичної інфраструктури» [4].

Хмарні технології стають дедалі більш поширеними в секторі кібербезпеки через свою спроможність гарантувати гнучкість, масштабованість і розподілену безпеку. Хмарні сервіси дають можливість організаціям зберігати й опрацьовувати інформацію у безпечних просторах, гарантуючи водночас захист від кібератак.

Одна з головних переваг застосування хмарних сервісів – змога втілення процедур резервного копіювання і відновлення інформації. У випадку кібератаки або якщо відбувся збій системи, інформація може бути оперативно відновлена без великих втрат. До того ж, хмарні провайдери, як правило, рекомендують сильні інструменти для того, щоб виявляти загрози і для моніторингу безпеки, що дає можливість організаціям сконцентруватися на ключових бізнес-процесах, залишивши управління безпекою спеціалістам.

Крім того, «хмарні технології забезпечують можливість централізованого управління безпекою, що дозволяє реалізувати спільні стратегії захисту для всіх підрозділів організації, що дозволяє вчасно виявляти та реагувати на загрози, підвищуючи загальний рівень захисту критичної інфраструктури» [4].

Управління ризиками та аналіз уразливостей вважаються основними складовими кібербезпеки, тому що вони дають можливість визначити, оцінити й мінімізувати ризики й вразливості, що здатні спричинити кібератаки й порушення безпеки. Зокрема:

1. Управління ризиками:

– «ідентифікація ризиків. Першим кроком управління ризиками є ідентифікація потенційних загроз та визначення можливих уразливостей у системах;

– оцінка ризиків. Після ідентифікації ризиків проводиться їх оцінка за ймовірністю та потенційним впливом на систему. Це допомагає визначити, які ризики потребують найбільшої уваги та заходів захисту;

– управління ризиками. Після оцінки ризиків визначаються стратегії зменшення чи управління ризиками. Це може включати уникнення ризиків, їх

прийняття, зменшення, перенесення чи управління ризиками через захисні заходи» [25].

2. Аналіз уразливостей:

– «систематичний огляд систем. Аналіз уразливостей включає детальний огляд системи для виявлення потенційних уразливостей та слабких місць, що можуть стати точками входу для потенційних атак;

– визначення й категоризація уразливостей. Цей процес визначає, які системи, програми чи процеси мають уразливості, а також їхні можливі наслідки. Уразливості розглядаються за потенційним впливом на безпеку систем;

– план заходів з усунення уразливостей. Після виявлення уразливостей розробляються стратегії для виправлення та усунення цих проблем, щоб зменшити можливість експлуатації цих ділянок системи;

– перевірка та оновлення. По завершенні усунення уразливостей системи регулярно перевіряються та оновлюються, щоб упевнитися у їхній безпеці та відсутності нових уразливостей» [25].

Управління ризиками та аналіз уразливостей є невід'ємним елементом частиною кібербезпеки. Вони дають можливість своєчасно встановлювати й ліквідувати потенційні проблеми, мінімізуючи загрози й поліпшуючи загальний ступінь захисту систем.

До того ж, «управління доступом та аутентифікація грають критичну роль у забезпеченні безпеки об'єктів критичної інфраструктури. Вони становлять важливі складові у проведенні контролю, хто має доступ до систем та даних, і як цей доступ здійснюється» [189]. Управління доступом охоплює формування і регулювання політик доступу до різних складових системи, що свідчить про визначення правил і обмежень для користувачів, в яких є доступ до відповідної інформації і ресурсів. Потрібно точно встановити рівні доступу й обмеження, аби мінімізувати ризик витоку даних або несанкціонованого втручання. У свою чергу, аутентифікація передбачає перевірку й підтвердження ідентичності користувачів перед тим, як надати доступ до

системи. Інноваційні методи аутентифікації застосовують не тільки паролі, а також і біометричну інформацію, двофакторну аутентифікацію й мультифакторні методи з метою гарантування безпеки.

Один із методів управління доступом – принцип найменших привілеїв, який вказує, що користувач отримує тільки ті права, що потрібні для здійснення його обов'язків, що сприяє обмеженню змог злочинців у випадку компрометації облікової інформації.

Одноразові паролі та застосування біометричних методів, як-от сканування відбитків пальців або розпізнавання обличчя, створюють належні умови для значного ступеня аутентифікації, тому що вони основуються на виняткових фізичних якостях користувачів.

У підсумку наведемо перелік основних інноваційних інструментів кіберзахисту на об'єктах критичної інфраструктури (див. табл. 3.5).

Таблиця 3.5

Основні інноваційні інструменти кіберзахисту на об'єктах критичної інфраструктури

Інноваційний інструмент	**Характеристика**	**Практичне значення для об'єктів критичної інфраструктури**
Системи виявлення загроз на основі штучного інтелекту та машинного навчання (AI/ML)	Дає змогу здійснити автоматизований аналіз великих масивів даних, виявити аномалії та невідомі атаки у реальному часі	Підвищує швидкість реагування на кіберінциденти, зменшує ризик масштабних збоїв
Платформи управління кіберінцидентами (SOAR, SIEM нового покоління)	Дозволяє інтегрувати збір, кореляцію та автоматизацію процесів реагування на кіберзагрози	Забезпечує централізоване управління безпекою та скорочує час ліквідації інцидентів
Технології Zero Trust	Створює умови для відмови від довіри за замовчуванням, постійної перевірки користувачів і пристроїв	Зменшує внутрішні загрози і ризики компрометації критичних систем
Хмарні та гібридні рішення кіберзахисту	Дає змогу використовувати хмарні сервіси для резервного зберігання, моніторингу та захисту даних	Забезпечує стійкість інфраструктури та безперервність функціонування сервісів
Автоматизовані системи резервного копіювання та відновлення (Disaster	Дозволяє швидко відновлювати дані і системи після кібератак або техногенних збоїв	Мінімізує простої і втрати у критично важливих галузях

Recovery, Backup as a Service)		
Кіберфізичні системи захисту промислових мереж (ICS/SCADA Security)	Створює умови для спеціалізованого захисту промислових та енергетичних систем управління	Запобігає порушенню технологічних процесів і фізичним аваріям
Технології блокчейн для забезпечення цілісності даних	Дає змогу децентралізовано зберігати інформацію	Захищає критичні дані від підроблення та несанкціонованого втручання
Кіберрозвідка	Допомагає збирати та аналізувати інформацію про стан актуальних та потенційних кіберзагроз	Створює умови доя проактивного управління кіберризиками та попереджує атаки
Цифрові двійники та симуляційні платформи	Створює умови для моделювання кіберінцидентів і тестування сценаріїв атак	Підвищує готовність до кризових ситуацій і навчання персоналу
VR/AR-тренінги з кібербезпеки	Дає змогу реалізації імерсивного навчання фахівців і операторів критичної інфраструктури	Формує практичні навички реагування на кіберінциденти

Джерело: власна розробка автора

Основний аналітичний фокус – практичне значення інноваційних інструментів, тому що якраз практична дієвість формує доречність застосування певних технологій в стратегічно значущих сферах. По-перше, інструменти на основі штучного інтелекту та машинного навчання гарантують якісно новий рівень реагування на кіберзагрози. Їх прикладна роль зводиться до спроможності викривати складні, до цього не знані види атак, не залучаючи людину, що насамперед значуще для об’єктів критичної інфраструктури, де затримка в реагуванні здатна спричинити каскадні відмови та масштабні соціально-економічні наслідки.

По-друге, платформи управління кіберінцидентами (SOAR, SIEM нового покоління) відіграють вирішальну роль для гарантування централізованого контролювання й координації дій у ході інцидентів. Їх введення дозволяє значно мінімізувати час фіксації загроз, покращити прозорість процедур управління безпекою і звести до мінімуму навантаження на працівників через автоматизацію стандартних операцій.

По-третє, концепція Zero Trust допомагає зменшенню ризиків несанкціонованого доступу до критичних систем, в тому числі на фоні

віддаленої роботи і розподілених мереж. Прикладна роль зазначеного інструмента зводиться до зменшення внутрішніх загроз та локалізації потенційних інцидентів, що дає можливість зберігати стабільність діяльності об’єктів навіть у випадку компрометації певних складових системи.

Вагоме значення мають хмарні та гібридні рішення кіберзахисту, що гарантують зростання стійкості інфраструктури й постійність надання послуг критичного характеру. Їхня прикладна значущість виражається в змозі оперативного масштабування потенцілу, географічної диверсифікації інформації та мінімізації ризиків знищення фізичним чином чи пошкодження серверних потужностей.

Особливу роль для критичної інфраструктури відіграють автоматизовані системи резервного копіювання і відновлення, що дають можливість звести до мінімуму простої після кібератак чи техногенних аварій. Прикладний результат подібних інструментів зводиться до збереження постійності життєво значущих процесів і зменшення фінансових та репутаційних втрат.

Спеціалізовані інструменти захисту промислових мереж (ICS/SCADA) націлені на те, щоб запобігти фізичним ефектам кібератак, в тому числі аваріям в секторі енергетики, транспорту або водопостачання. Їхня практична роль зводиться до захисту технологічних процесів, від стабільності котрих прямо залежить безпека громадян і діяльність держави.

Застосування технологій блокчейн з метою гарантування цілісності інформації дає змогу збільшити ступінь довіри до інформаційних систем критичної інфраструктури. Практична значущість подібних рішень зводиться до неспроможності прихованої зміни чи підробки критичної інформації, що вважається насамперед вагомим у державному управлінні, а також фінансовій сфері.

Платформи кіберрозвідки гарантують перехід від реактивної до проактивної моделі кіберзахисту. Їхня практична роль зводиться до вчасного викриття ймовірних загроз, передбачення атак та ухвалення превентивних управлінських рішень, що значно мінімізує загальний рівень кіберризиків.

Інноваційні цифрові двійники та симуляційні платформи дають можливість моделювати наслідки кібератак, не втручаючись у реальні системи. Прикладний результат їх використання зводиться до збільшення готовності організацій до кризових ситуацій, відпрацювання алгоритмів реагування й оптимізації управлінських рішень.

Врешті-решт, VR/AR-тренінги з кібербезпеки відіграють істотну прикладну роль для вироблення професійних компетентностей працівників об’єктів критичної інфраструктури. Імерсивні навчальні простори дають можливість здійснювати відпрацювання дій в обставинах, які по-максимуму наближені до реальних кібератак, завдяки чому зростає результативність людського фактора як однієї з головних складових системи кіберзахисту.

Розгляд практичної ролі інноваційних інструментів кіберзахисту вказує, що їхнє введення в комплексі гарантує зростання кіберстійкості об’єктів критичної інфраструктури, зменшення негативних ефектів кібератак і формування умов для стабільної діяльності критично значущих систем на фоні зростаючих загроз.

Явно помітно, що кібербезпека потребує безперервного еволюційного підходу, щоб дієво протидіяти нинішнім і майбутнім кіберзагрозам. Одержані підсумки акцентують на декількох основних чинниках. Новітня кіберзагроза безперервно збільшується за своєю складністю й масштабом. Викриття і протидія таким загрозам потребує не лише інновацій технічного характеру, а також стратегічного перегляду підходів до кіберзахисту. Впровадження інноваційних інструментів, зокрема штучного інтелекту, блокчейн-технологій та машинного навчання, володіє значним потенціалом для зростання результативності заходів кіберзахисту. Зростання і вдосконалення таких технологій – вагоме завдання для перспективи. Реального успіху в кіберзахисті можна досягти тільки шляхом комплексного підходу, котрий бере до уваги технічні, організаційні й людські чинники. Співробітництво між усіма сторонами, включно з урядовими органами, приватною сферою і громадянським суспільством, встановлюється як головна складова вдалої

стратегії. Навчання й освіта у секторі кібербезпеки відіграють вирішальну роль. Зростання ступеня усвідомлення й навичок в секторі кіберзахисту з-поміж усього персоналу, від технічних фахівців до керівних кадрів, буде сприяти загальному зростанню ступеня кібербезпеки

Згадані інструменти сприяють ускладненню процедури несанкціонованого доступу до систем, однак їхня результативність потребує безперервного оновлення і вдосконалення. Приміром, використання шифрування даних у ході передавання і збереження і, крім того, систематичне оновлення програмного забезпечення сприяють у зростанні рівня безпеки. Всі зазначені заходи націлені на гарантування значного ступеня захисту критичних систем й інформації. Правильне управління доступом й дієва аутентифікація – вагомі складові для запобігання несанкціонованому доступу й збереженню даних у безпеці.

Висновки до розділу 3

1. Систематизація зарубіжних підходів до формування й упровадження механізмів реалізації публічної політики у сфері кібербезпеки дозволили окреслити ключові вектори вдосконалення національної системи в Україні. До таких пріоритетів належать: розширення та впорядкування доступу до інформаційних даних; формування потужного національного кібернетичного ресурсу; цілеспрямоване використання інформаційних активів в інтересах держави; розбудова комплексної системи захисту даних; активізація міжнародного співробітництва у сфері інформаційної та кібербезпеки; забезпечення інформаційного суверенітету держави; модернізація та розвиток кібернетичної інфраструктури.

2. Запропоновано комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України, метою якого є формування цілісної, адаптивної та стійкої системи публічного управління кібербезпекою, здатної забезпечити належний рівень захисту національних

інформаційних ресурсів, критичної інформаційної інфраструктури та суспільних інтересів від сучасних і перспективних кіберзагроз шляхом удосконалення нормативно-правових, організаційних та інформаційно-технічних інструментів управління. Серед очікуваних результатів окреслено наступні: формування цілісної та узгодженої системи публічного управління кібербезпекою; підвищення ефективності координації та міжвідомчої взаємодії; зміцнення кіберстійкості держави та критичної інформаційної інфраструктури; підвищення рівня правової визначеності та адаптивності регулювання; посилення інформаційно-технічних та аналітичних спроможностей; активізація публічно-приватного та міжнародного співробітництва; підвищення готовності до реагування на гібридні та воєнні кіберзагрозию.

3. З'ясовано, що інноваційні інструменти кіберзахисту є головним фактором гарантування стабільності й надійності діяльності об’єктів критичної інфраструктури на фоні безперервного ускладнення кіберзагроз. Їхня прикладна роль зводиться не тільки до технічного протистояння кібератакам, а також до створення цілісної системи управління кіберризиками, котра включає превентивні, реактивні й відновлювальні заходи. Використання таких інструментів дає можливість зменшити вірогідність масштабних збоїв, обмежити каскадний ефект інцидентів й гарантувати постійність надання критично значущих послуг громадянам та державі. До основних інструментів віднесено: системи виявлення загроз на основі штучного інтелекту та машинного навчання (AI/ML); платформи управління кіберінцидентами (SOAR, SIEM нового покоління); технології Zero Trust; хмарні та гібридні рішення кіберзахисту; автоматизовані системи резервного копіювання та відновлення (Disaster Recovery, Backup as a Service); кіберфізичні системи захисту промислових мереж (ICS/SCADA Security); технології блокчейн для забезпечення цілісності даних; кіберрозвідка та Threat Intelligence-платформи; цифрові двійники та симуляційні платформи; VR/AR-тренінги з кібербезпеки. В той же час якнайкращого результату від інноваційних інструментів можна

досягти в разі їхнього комплексного введення, беручи до уваги галузеву своєрідність, ступінь цифрової зрілості організацій й кадрових ресурсів. Синтез технологічних інновацій зі зростанням компетентностей працівників, новітніми управлінськими підходами й державною політикою в секторі кібербезпеки формує підгрунтя для зростання кіберстійкості критичної інфраструктури у довгостроковому майбутньому й посилення національної безпеки в цілому.

ВИСНОВКИ

У дисертаційному дослідженні вирішено важливу наукову проблему, яка полягає в теоретичному обґрунтуванні засад публічного управління у сфері забезпечення кібербезпеки та розробленні практичних рекомендацій щодо розвитку механізмів його реалізації в сучасних умовах, відповідно до чого сформульовано такі висновки та рекомендації.

1. Охарактеризовано глобальні тенденції та виклики у сфері забезпечення кібербезпеки, серед яких виділено: зростання кількості та складності кібератак, мілітаризація кіберпростору, діджиталізація критичної інфраструктури, поширення IoT та кіберфізичних систем, хмарна трансформація та ризики зберігання даних, недостатня цифрова грамотність населення, кадровий дефіцит кіберфахівців, політизація та фрагментація кіберпростору, зростання кіберзлочинності та тіньових кіберринків, виклики регулювання штучного інтелекту, проблеми захисту персональних даних, дезінформація та інформаційні операції. Новітнім глобальним тенденціям у сфері кібербезпеки властиві комплексність, багаторівневість й асиметричність, виражаючи нерівномірність цифрового зростання різних груп держав і своєрідність їх політичних, економічних та технологічних змог.

2. Вивчено сутність та зміст публічного управління у сфері забезпечення кібербезпеки. На основі аналізу підходів науковців до розуміння сутності даного поняття запропоновано більш сучасне та актуальне визначення даного поняття. На наш погляд, під публічним управлінням у сфері забезпечення кібербезпеки варто розуміти цілеспрямовану, скоординовану та інноваційно орієнтовану діяльність, яка здійснюється органами державної влади, органами місцевого самоврядування та іншими суб’єктами публічної влади, на яку покладено завдання формувати, реалізовувати та оцінювати політики кіберзахисту, забезпечувати кіберстійкість держави, захист цифрового суверенітету, критичної інфраструктури й інформаційного простору, використовуючи нормативно-правові, організаційні, інформаційно-

технологічні механізми у взаємодії з приватним сектором, громадянським суспільством та міжнародними інституціями.

3. Досліджено цифровізацію публічного управління як каталізатор розвитку кібербезпеки та ризик-менеджменту у цій сфері та виявлено, що цифровізація публічного управління являє собою застосування цифрових технологій і потенціалу онлайн-комунікацій під час ухвалення і виконання публічних управлінських рішень, надання адміністративних послуг і, крім того, створення дієвих інструментів введення державної політики в усіх секторах життя суспільства. Цифрові технології орієнтовані на якнайбільше зменшення часу передавання інформаційних повідомлень від державних органів до кінцевих користувачів шляхом ефективного застосування цифрового простору. По-перше, це робить простішим процес одержання важливих публічних послуг і дозвільної документації для людей, по-друге, мінімізує фінансові витрати на обслуговування системи надання публічних послуг в офлайн-режимі, та, по-третє, зменшує вияви корупції, тому що немає прямого контакту між надавачем публічних послуг і громадянином. Синергетичні можливості соціальних, мобільних, хмарних технологій, технологій вивчення інформації й Інтернету речей спільно мають ресурс спричиняти трансформаційні зміни в державному управлінні і загалом встановити його результативність, реактивність і цінність.

4. Проаналізовано механізми публічного управління у сфері забезпечення кібербезпеки України, в результаті чого зроблено висновок про утворення комплексної, багатоступеневої системи державного реагування на новітні кіберзагрози. Нормативно-правове забезпечення започатковує базові принципи державної політики в секторі кібербезпеки, встановлює коло суб’єктів, їх повноваження і процеси взаємодії і, крім того, гарантує інтеграцію національного законодавства з міжнародними і європейськими стандартами. Організаційне забезпечення публічного управління у сфері кібербезпеки основується на функціонуванні системи спеціальних державних органів і координаційних інституцій, що гарантують стратегічне планування,

міжвідомчу взаємодію і реагування на кіберінциденти. Інформаційно-технічне забезпечення є інфраструктурним базисом публічного управління в секторі кібербезпеки, гарантуючи діяльність державних інформаційних систем, здійснення моніторингу кіберзагроз, захист інформаційних ресурсів та сприяння управлінським рішенням.

5. Оцінено сучасний стан та проблеми реалізації публічного управління у сфері забезпечення кібербезпеки України. Ефективність реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України доречно досліджувати в розрізі сильних сторін, що утворилися останніми роками. Передусім мова йде про існування базового нормативно-правового і стратегічного підґрунтя, що формує цілі, принципи та суб'єктів державної політики в секторі кібербезпеки. Крім того, вагома перевага – інституційна фіксація відповідальності за координацію і реагування на кіберзагрози, і, до того ж, нагромаджений практичний досвід протидії масштабним кібератакам на тлі гібридної і повномасштабної війни. Додатковий фактор зростання результативності – активне міжнародне співробітництво і сприяння зі сторони стратегічних партнерів, що допомагає посилити кіберстійкість державної сфери. Водночас реалізація механізмів публічного управління у сфері кібербезпеки супроводжується низкою системних слабких сторін. З-поміж них основними продовжують залишатися фрагментарність повноважень між різними органами влади, недостатній ступінь міжвідомчої координації, а також нерівномірність введення заходів кіберзахисту на центральному й місцевому рівнях. Велика проблема – брак кваліфікованого персоналу й, крім того, обмежений фінансовий й матеріально-технічний потенціал, через що ускладнюється практична імплементація стратегічних документів та погіршується загальна ефективність державної політики в згаданій галузі. Публічне управління у сфері забезпечення кібербезпеки України функціонує в умовах підвищеної системної напруженості, зумовленої поєднанням внутрішніх управлінських дисфункцій і зовнішніх викликів воєнного характеру, що проявляється у фрагментованості інституційної архітектури та

нечіткості розмежування повноважень між суб'єктами публічної влади, недостатній міжвідомчій координації, неповноті й неузгодженості нормативно-правового забезпечення та його обмеженій гармонізації зі стандартами ЄС і НАТО, дефіциті кваліфікованих кадрів і слабкій управлінській складовій системи професійної підготовки, обмеженості фінансових, технічних і інфраструктурних ресурсів, нерозвиненості механізмів публічно-приватного партнерства, низькому рівні цифрової обізнаності населення, реактивному характері управління, недостатності стратегічного прогнозування й ризик-менеджменту, а також у нових проблемах, спричинених повномасштабною агресією РФ, зокрема різкому зростанні масштабів і складності кібератак, перевантаженні та вразливості державних інформаційних систем, порушенні стабільності міжвідомчої взаємодії, посиленні залежності від міжнародної технічної допомоги та інтеграції кіберзагроз з інформаційно-психологічним впливом, що в сукупності знижує адаптивність і стійкість національної системи кібербезпеки.

6. Систематизація зарубіжних підходів до формування й упровадження механізмів реалізації публічної політики у сфері кібербезпеки дозволили окреслити ключові вектори вдосконалення національної системи в Україні. До таких пріоритетів належать: розширення та впорядкування доступу до інформаційних даних; формування потужного національного кібернетичного ресурсу; цілеспрямоване використання інформаційних активів в інтересах держави; розбудова комплексної системи захисту даних; активізація міжнародного співробітництва у сфері інформаційної та кібербезпеки; забезпечення інформаційного суверенітету держави; модернізація та розвиток кібернетичної інфраструктури.

7. Запропоновано шляхи удосконалення механізмів публічного управління у сфері забезпечення кібербезпеки України, у контексті чого запропоновано комплексний механізм удосконалення публічного управління у сфері забезпечення кібербезпеки України, метою якого є формування

цілісної, адаптивної та стійкої системи публічного управління кібербезпекою, здатної забезпечити належний рівень захисту національних інформаційних ресурсів, критичної інформаційної інфраструктури та суспільних інтересів від сучасних і перспективних кіберзагроз шляхом удосконалення нормативно-правових, організаційних та інформаційно-технічних інструментів управління. Серед очікуваних результатів окреслено наступні: формування цілісної та узгодженої системи публічного управління кібербезпекою; підвищення ефективності координації та міжвідомчої взаємодії; зміцнення кіберстійкості держави та критичної інформаційної інфраструктури; підвищення рівня правової визначеності та адаптивності регулювання; посилення інформаційно-технічних та аналітичних спроможностей; активізація публічно-приватного та міжнародного співробітництва; підвищення готовності до реагування на гібридні та воєнні кіберзагрози.

8. Розроблено напрями розвитку інноваційних інструментів кіберзахисту на об’єктах критичної інфраструктури. Використання таких інструментів дає можливість зменшити вірогідність масштабних збоїв, обмежити каскадний ефект інцидентів й гарантувати постійність надання критично значущих послуг громадянам та державі. До основних інструментів віднесено: системи виявлення загроз на основі штучного інтелекту та машинного навчання (AI/ML); платформи управління кіберінцидентами (SOAR, SIEM нового покоління); технології Zero Trust; хмарні та гібридні рішення кіберзахисту; автоматизовані системи резервного копіювання та відновлення (Disaster Recovery, Backup as a Service); кіберфізичні системи захисту промислових мереж (ICS/SCADA Security); технології блокчейн для забезпечення цілісності даних; кіберрозвідка та Threat Intelligence-платформи; цифрові двійники та симуляційні платформи; VR/AR-тренінги з кібербезпеки. В той же час якнайкращого результату від інноваційних інструментів можна досягти в разі їхнього комплексного введення, беручи до уваги галузеву своєрідність, ступінь цифрової зрілості організацій й кадрових ресурсів. Синтез технологічних інновацій зі зростанням компетентностей працівників,

новітніми управлінськими підходами й державною політикою в секторі кібербезпеки формує підґрунтя для зростання кіберстійкості критичної інфраструктури у довгостроковому майбутньому й посилення національної безпеки в цілому.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Абрат С. Б. Співробітництво ЄС та країн-учасниць Східного партнерства у сфері кібербезпеки: виклики та перспективи. Міжнародні та політичні дослідження. 2024. Вип. 37. С. 171-178.

2. Алексєєв М.М. Аналіз методологічних підходів щодо застосування технологій управління ризиками у сфері кібербезпеки. Modern Information Technologiesinthe Sphere of Security and Defence. 2019. № 1(34). С. 109-114.

3. Алієв А. Цифровізація публічного управління у сфері національної безпеки: світові тенденції та рекомендації для України. Таврійський науковий вісник. Серія: Економіка, 2025. Вип. 25, С. 170-178. https://doi.org/10.32782/2708-0366/2025.25.18.

4. Андрух А., Юрченко Ю. Кібербезпека критичної інфраструктури: виклики інновацій і загрози цифрових технологій. Challenges and Issues of Modern Science. 2024. Vol. 3. С. 157-166.

5. Арпентій С. П. Стратегічні засади забезпечення кібербезпеки США. Інформація і право. 2025. № 2. С. 176-182.

6. Арсенович Л. Парадигма захисту критичної інфраструктури в системі національної безпеки України. Державне управління: удосконалення та розвиток. 2024. № 8. URL: https://www.nayka.com.ua/index.php/dy/article/view/4404/4439.

7. Арсенович Л. Сутність кібербезпеки як напряму вироблення державної політики цифрового розвитку. Ефективність державного управління. 2021. Вип. 3-4. С. 9-21.

8. Атаманова Н., Луняченко І. До питання цифровізації публічного управління в Україні. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2024. № 68. С. 4-11.

9. Бабанін С. Кіберзлочинність, Комп’ютерна злочинність. Велика українська юридична енциклопедія : у 20 т. Харків. 2019. Том 18. с. 207

10. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. Підприємництво, господарство і право. 2019. № 9. С. 102.

11. Берназюк О. Цифрові технології у праві: тенденції та перспективи розвитку : дис. д-ра юрид. наук: 12.00.07. Ужгород. 2021. с. 45-52.

12. Бигаса Ю., Бєлов Д., Заборовський В. Штучний інтелект та авторські і суміжні права. Науковий вісник Ужгородського Національного університету.2023. URL: https://doi.org/10.24144/2307-3322.2022.76.2.47.

13. Блистів Т., Колесник В. Захист критичної інфраструктури як фундамент загальноєвропейської безпеки. Сучасні аспекти реформування системи публічного управління в умовах воєнного часу : матеріали І Міжнар. наук.-практ. конф. Переяслав. 2023. С. 31.

14. Бондаренко М. Кіберзагрози в національній безпеці та роль державних органів у їх нейтралізації. Харків: ХНУВС. 2018. С. 176.

15. Бондарчук О. І., Науменко Т.С., Товт Б.М. Розробка та впровадження інноваційних методів кібербезпеки у комп'ютерних системах. Таврійський науковий вісник. Серія : Технічні науки. 2024. Вип. 4. С. 31-40.

16. Вдовенко С., Даник Ю., Фараон С. Дефініційні проблеми термінології у сфері кібербезпеки і кібероборони та шляхи їх вирішення. Комп'ютерні науки та кібербезпека. 2019. №1. С.18-30.

17. Веселова Л. Особливості державної політики України у сфері забезпечення кібербезпеки в умовах гібридної війни. Науковий вісник Херсонського державного університету. Серія: «Юридичні науки». 2019. № 2. С. 25.

18. Вівчар І. Кібербезпека як сфера міжнародного співробітництва в період глобальної кризи безпеки. Вісник Національного юридичного університету імені Ярослава Мудрого. Серія : Філософія, філософія права, політологія, соціологія. 2025. № 2. С. 122-143.

19. Вовк А. Сучасні проблеми публічного управління забезпеченням кібербезпеки в Україні. Публічне управління: концепції, парадигма, розвиток,

удосконалення. 2024. №8. С. 28–35. URL: https://doi.org/10.31470/ 2786- 6246-2024-8-28-35.

20. Вознюк Є., Андрюхіна В. Порівняльний аналіз кібербезпеки Європейського Союзу. Міжнародні відносини, суспільні комунікації та регіональні студії. 2025. № 2. С. 136-154.

21. Гавриляк В. Стратегія кібербезпеки ЄС на цифрове десятиліття: перспективи для України. Вісник Національної академії державного управління при Президентові України. Серія: Державне управління. 2021. №1. С. 46-52.

22. Гаврись А., Філіппова В., Тур Н. Інформаційний аналіз систем захисту об'єктів критичної інфраструктури в період дії воєнного стану. Вісник Львівського державного університету безпеки життєдіяльності. 2024. № 30. С. 173.

23. Герасимюк К. Механізми державного управління кібер- та інформаційною безпекою: проблеми та шляхи вирішення. Публічне управління та адміністрування. 2021. №3. URL: https://dspace.vnmu.edu.ua/xmlui/handle/123456789/9519?locale-attribute=en.

24. Геращенко Ю. Державна політика у сфері кібербезпеки в Україні. Вчені записки ТНУ імені В.І. Вернадського. Серія: «Державне управління». 2019. № 1. С. 141.

25. Гнатюк С., Бердибаєв Р., Сидоренко В., Жигаревич О., Смірнова Т. Система корелювання подій та управління інцидентами кібербезпеки на об’єктах критичної інфраструктури. Кібербезпека: освіта, наука, техніка. 2023. №3(19). С. 176-196.

26. Горєлова В. Кібербезпека: виклики цифрової ери через призму Конгресу ООН У КІОТО. Legal Bulletin. 2024. (№14). С. 98-104.

27. Горлинський В., Горлинський Б. Освітні пріоритети підготовки фахівців з кібербезпеки в умовах воєнного стану в державі. Information Technology and Security. 2024. Vol. 12, Iss. 2. С. 268-282.

28. Горун О. Пріоритетні засади державної політики кібербезпеки: організаційно-правовий аспект. Інформація і право. 2021. № 2 (37). С. 95.

29. Горун О. Ю. Правове забезпечення національної системи кібербезпеки. Інформація і право. 2024. № 4. С. 123-132.

30. Грайворонський М. Сучасні підходи до забезпечення кібернетичної безпеки. Матеріали XIII Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих вчених «Теоретичні і прикладні проблеми фізики, математики та інформатики». м. Київ. 21-23 травня 2015. Київ : НТУУ «КПІ». 2015. С.17.

31. Грень Л. М., Грибко О. В. Гарантування кібербезпеки в умовах цифровізації соціальної сфери. Вісник Національного технічного університету «ХПІ». Серія : Актуальні проблеми розвитку українського суспільства. 2025. № 1. С. 45-53.

32. Грищенко С. М. Правове регулювання кібербезпеки в умовах цифрової трансформації суспільства. Інформація і право. 2025. № 3. С. 122-130.

33. Давидюк А. Система обміну знаннями та досвідом між фахівцями з кібербезпеки критичної інфраструктури. Науково-практична конференція «Кібербезпека енергетики». Матеріали. 2023. С. 67-73.

34. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Одеса: ОНАЗ, 2019. 320 с.

35. Демедюк С. В., Користін О.Є. Стійкість системи кібербезпеки та її забезпечення в НАТО. Наука і правоохорона. 2023. № 1. С. 77-85.

36. Державна служба спеціального зв’язку та захисту інформації України. Офіційний сайт. URL: https://cip.gov.ua/ua.

37. Державний центр кіберзахисту. Офіційний сайт. URL: https://scpc.gov.ua/uk.

38. Деякі питання забезпечення функціонування системи виявлення вразливостей і реагування на кіберінциденти та кібератаки: Постанова

Кабінету Міністрів України; Порядок від 23.12.2020 № 1295. URL: https://zakon.rada.gov.ua/laws/show/1295-2020-%D0%BF#Text.

39. Деякі питання об'єктів критичної інформаційної інфраструктури: Постанова Кабінету Міністрів України від 09.10.2020 № 943. URL: https://zakon.rada.gov.ua/laws/show/943-2020-%D0%BF#Text.

40. Дзеньків В. Кібербезпека в умовах сучасних загроз: ізраїльський досвід і його застосування в Україні. Науковий вісник Ужгородського національного університету. Серія ПРАВО. 2024. Вип. 84. Ч. 3. С. 79.

41. Дзяна Г., Дзяний Р. Система публічного управління як об’єкт критичної інфраструктури. Європейська інтеграція та трансформація публічного врядування в Україні: матер. наук.-практ. конф. Львів: НУ «Львівська політехніка». 2024. С. 111-114.

42. Дмитрів С., Пікалюк С. Профілактика кіберзлочинів в умовах цифровізації державного управління та бізнесу. Науковий вісник Ужгородського Національного університету. Серія право. 2025. Випуск 87: частина 3. URL: https://doi.org/10.24144/2307-3322.2025.87.3.41.

43. Довгань О. Д., Ткачук Т.Ю. Правові аспекти забезпечення кібербезпеки об’єктів критичної інфраструктури: національний та міжнародний вимір. Інформація і право. 2024. № 4. С. 113-122.

44. Доценко Т. В., Кузьменко М.В. Зрілість системи кібербезпеки країни в умовах війни: тенденції оцінювання. Економічний вісник Дніпровської політехніки. 2024. № 3. С. 34-43.

45. Дубовик В. Б. Роль ОБСЄ у забезпеченні кібербезпеки. Юридичний бюлетень. 2020. Вип. 12. С. 87-91.

46. Дяченко В. Особливості формування кібербезпеки в умовах сучасних викликів. Управління економікою: теорія та практика. Чумаченківські читання. 2024. С. 242-248.

47. Дяченко В., Дяченко Н. Врахування ризиків при використанні інформаційних технологій. Information technology: computer science, software engineering and cyber security. 2024. Вип. 4. С. 75-80.

48. Живило Є. О. Методологія розробки національної стратегії кібербезпеки. Державне будівництво. 2024. № 2. С. 307-321.

49. Живило Є. О. Пріоритетні напрями національної стратегії кібербезпеки в контексті інтеграції до трирівневої моделі кібероборони. Державне будівництво. 2025. № 1. С. 229-252.

50. Живило Є. О. Шляхи врегулювання нормативно-правової бази із захисту інформації, кібербезпеки та кібероборони України. Публічне адміністрування та національна безпека. 2019. № 3. С. 7-11.

51. Журило О., Ляшенко О., Аветісова К. Огляд рішень з апаратної безпеки кінцевих пристроїв туманних обчислень у Інтернеті речей. Сучасний стан наукових досліджень та технологій в промисловості. 2023. №1(23). С. 57-71. URL: https://doi.org/10.30837/ITSSI.2023.23.057.

52. З початку 2025-го в Україні фіксується близько 15 кібератак щодня. URL: https://suspilne.media/1075891-z-pocatku-2025-go-v-ukraini-fiksuetsa-blizko-15-kiberatak-sodna-derzspeczvazku.

53. Завгородня Ю. В. Державна політика в сфері кібербезпеки в умовах повномасштабної війни. Актуальні проблеми політики. 2024. Вип. 74. С. 62-66.

54. Завербний А. С. Особливості формування системи управління кібербезпекою підприємств у воєнний період: теоретико-прикладний аспект. Innovation and Sustainability. 2024. Iss. 1. С. 13-21.

55. Загорняк В. Дослідження механізмів захисту від соціально-інженерних атак та розробка методів їх виявлення. 2023. URL: https://elartu.tntu.edu.ua/bitstream/lib/41860/2/Dyplom_Zahornyak_V_Y_2023.pdf.

56. Зінченко О. І. Вплив політичної ситуації в Україні на проблеми кібербезпеки Європейського регіону. Політикус. 2024. Вип. 5. С. 154-158.

57. Зінченко О. І. Кібербезпека як елемент демократичної консолідації: уроки Харківщини. Вісник Харківського національного університету імені В. Н. Каразіна. Серія : Питання політології. 2025. Вип. 47. С. 46-52.

58. Зуй В. В. Актуальні проблеми кібербезпеки в Україні з урахуванням європейської інтеграції. Південноукраїнський правничий часопис. 2022. №4(1). С. 231-235.

59. Іваненко Р. О. Інтеграція штучного інтелекту в системи кібербезпеки: можливості та виклики. Ukrainian Journal of Computing Innovations. 2024. Вип. 1. URL: http://nbuv.gov.ua/UJRN/ujci_2024_1_7.

60. Іваночко Т. А., Семенюк С.А. Управління ризиками кібербезпеки з використанням NIST CSF 2.0. Сучасний захист інформації. 2025. № 3. С. 75-82.

61. Кабінет Міністрів України. Офіційний сайт. URL: https://www.kmu.gov.ua.

62. Кавин С. Я. Правові засади забезпечення кібербезпеки в державах – членах Європейського Союзу. Актуальні проблеми держави і права. 2020. Вип. 87. С. 51-58.

63. Кагарлицький Р. Біометрична автентифікація користувача смартфона за допомогою даних акселерометра. 2023. URL: https://ela.kpi.ua/bitstream/123456789/60442/1/Kaharlytskyi_bakalavr.pd.

64. Казьмірук С. Забезпечення кібербезпеки об’єктів критичної інфраструктури на основі використання штучного інтелекту в умовах воєнного стану. Юридичний науковий електронний журнал. 2024. №6. С. 201-205.

65. Карвацька С. Б., Маник А.З., Строїч М.І. Кібербезпека: сучасні виклики та міжнародно-правові рамки щодо захисту даних. Науковий вісник Ужгородського національного університету. Серія : Право. 2025. Вип. 87(4). С. 251-256.

66. Кібербезпека в інформаційному суспільстві: Інформаційно-аналітичний дайджест. Державна наукова установа «Інститут інформації, безпеки і права НАПрН України». К.2023. №9. 351 с.

67. Кібербезпека в Україні 2025: виклики та перспективи. URL: https://galera.news/kiberbezpeka-v-ukrayini-2025-vyklyky-ta-perspektyvy-7009.

68. Кібербезпека: українські реалії. URL: http://timeua.info/post/oborona-i-bezopasnost/k-berbezpeka-ukra-ns-k--real-- 07454.html.

69. Кібербезпека: як захистити підприємство в епоху Індустрії X.0. URL: https://www.telesphera.net/blog/kiberbezpeka- indystrii-x-0.html.

70. Кількість кібератак на Україну зросла на 70% за рік: головні мішені хакерів. URL: https://epravda.com.ua/tehnologiji/kilkist-kiberatak-na-ukrajinu-zrosla-na-70-za-rik-golovni-misheni-hakeriv-801807.

71. Книш З. І. Кібербезпека: актуальний стан нормативно-правової бази та перспективи її розвитку. Історико-правовий часопис. 2025. № 1. С. 59-65.

72. Коваленко Н., Панасюк І. Управління ризиками транснаціональних корпорацій. Економіка та менеджмент кораблебудування. 2020. №4. С. 103-109.

73. Коваль І. М., Головня С.А. Особливості створення багаторівневої моделі кібербезпеки даних критичної інфраструктури: міждисциплінарний підхід. Комп'ютерно-інтегровані технології: освіта, наука, виробництво. 2024. № 57. С. 57-68.

74. Козьміних А. В., Прохоренко А.М. Загальна характеристика особливостей та проблем кібербезпеки в сучасній Україні. Актуальні проблеми політики. 2022. Вип. 70. С. 101-105.

75. Комітет з питань свободи слова. URL: https://komsvobslova. rada.gov.ua.

76. Кондратьєв В. Ю. Розвиток кібербезпеки у світі: друга половина XX століття. Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія : Історичні науки. 2025. Т. 36(75), № 1. С. 368-373.

77. Конюхов Б. Виклики кібербезпеки в управлінні інформаційними ресурсами в системі державного управління. Молодіжний соціологічний форум НТУ «ХПІ». 2024. URL: https://repository.kpi.kharkov.ua/bitstreams/a04a3511-7c5e-4e87-83ad-a6675fae2480/download.

78. Костенко В. О., Кринична І.П., Журбинський Д.А. Актуальність посилення кібербезпеки України в умовах дії воєнного стану в контексті

європейської інтеграції. Публічне управління і адміністрування в Україні. 2023. Вип. 34. С. 74-77.

79. Костенко І. В., Оксінь В.Ю., Левченко Д.С. Державно-приватне партнерство у сфері кібербезпеки як інструмент забезпечення національної безпеки: адміністративно-правовий аспект. Наука і техніка сьогодні. Серія: Педагогіка; Право; Економіка; Фізико-математичні науки; Техніка. 2025. № 11. С. 175-188.

80. Костенко О. В. Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі. Інформація і право. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Київ, 2019. № 3 (30). С. 96-104.

81. Котух В. Формування систем кібербезпеки в органах публічної влади. URL: https://www.researchgate.net/profile/Yevgeniy-Kotukh-2/publication/340234957_formation_of_cyber_security_systems_in_public_authorities/links/604f6bf992851cd8ce427bab/formation-of-cyber-security-systems-in-public-authorities.pdf

82. Котух Є. В. Особливості забезпечення кібербезпеки в публічному секторі в умовах глобалізації. Державне будівництво. 2019. № 2. URL: http://nbuv.gov.ua/UJRN/DeBu_2019_2_18.

83. Кочман К. Міжнародний досвід адміністративно-правового забезпечення протидії кіберзагрозам. Південноукраїнський правничий часопис. 2025. № 1. С. 107-112.

84. Круглов В. Державно-приватне партнерство у сфері кібербезпеки. Вчені записки ТНУ ім. В.І. Вернадського. Серія: «Державне управління». 2018. № 3. Т. 29(68). С. 57-61.

85. Крушеніцький В. Зарубіжний досвід забезпечення національної безпеки у публічно-інформаційній сфері. Науковий вісник Сіверщини. Серія: Право. 2025. № 3 (26). С. 19-28.

86. Кубанов Є. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління. Аспекти публічного управління. 2018. Т. 6. № 8. С. 51.

87. Лазарів В. Кібербезпека та публічне управління: виклики та можливості для електронних послуг. Актуальні питання у сучасній науці. 2025. №1 (31). С. 281-291.

88. Ларін С. Захист інформації в системі кібербезпеки як стратегічний пріоритет реалізації державних механізмів захисту національних цінностей в Україні. Публічне управління та регіональний розвиток. 2025. № 27. С. 278-294.

89. Лисеюк А. М., Свінцицька Т.В. Правове забезпечення кібербезпеки України в умовах воєнного стану та євроінтеграції. Право та інновації. 2024. № 4. С. 32-38.

90. Лисеюк А. М., Свінцицька Т.В. Розвиток міжнародного співробітництва у сфері кібербезпеки: нормативно-правові засади та перспективи. Право та інноваційне суспільство. 2024. № 2. С. 89-95.

91. Лук’янчук Р. Державне управління кібернетичною безпекою: шляхи вдосконалення в сучасних умовах. Державне управління: удосконалення та розвиток. 2015. № 9. URL: http://nbuv.gov.ua/UJRN/Duur_2015_9_17.

92. Мазепа С. О. Кібербезпека в Україні: сучасні виклики та шляхи вдосконалення законодавчого регулювання. Актуальні проблеми правознавства. 2025. Вип. 2. С. 164-171.

93. Мамедова Е. А. Сучасна концепція правового регулювання кібербезпеки в Україні. Юридичний бюлетень. 2021. Вип. 22. С. 131-140.

94. Мануілов Я. С. Європейський досвід забезпечення кібербезпеки. Інформація і право. 2025. № 2. С. 147-154.

95. Мельник Д. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи їх вирішення. Адміністративне право і процес. 2022. №3(38). С. 5–16. URL: https://doi.org/10.17721/2227-796X.2022.3.01.

96. Мельник О. Публічне управління в сфері кібербезпеки: теоретичні засади та практичні аспекти. Київ: Інститут публічного управління. 2019. С. 298.

97. Мельничук О. Управління критичною інфраструктурою: модель та її впровадження. Актуальні проблеми державного управління. 2020. № 1(81). С. 64.

98. Міністерство закордонних справ України. Офіційний сайт. URL: https://mfa.gov.ua.

99. Міністерство оборони України. Офіційний сайт. URL: https://mod.gov.ua.

100. Мялковський Д. В. Організаційно-правові механізми державного управління міжнародним співробітництвом України у сфері кібербезпеки. Теорія та практика державного управління. 2019. Вип. 3. С. 216-226.

101. Найпоширеніші види кіберзлочинів у 2024 році. URL: https://galera.news/najposhyrenishi-vydy-kiberzlochyniv-u-2024-rotsi-3637.

102. Науково-практичний коментар до Положення про організаційно-технічну модель кіберзахисту, затвердженого постановою Кабінету Міністрів України від 29.12.2021 № 1426. Державна служба спеціального зв'язку та захисту інформації. URL: https://cip.gov.ua/ua/news/naukovo-praktichnii-komentar-do-polozhennya-pro-organizaciino-tekhnichnu-model-kiberzakhistu-zatverdzhenogo-postanovoyu-kabinetu-ministriv-ukrayini-vid-29-grudnya-2021-r-1426.

103. Національна поліція України. Офіційний сайт. URL: https://npu.gov.ua.

104. Національний банк України. Офіційний сайт. URL: https://bank.gov.ua.

105. Національний координаційний центр кібербезпеки. Офіційний сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/3303.html.

106. Огляд ринку кібербезпеки в Україні Січень 2025. URL: https://itukraine.org.ua/files/Ukraine-Cybersec-Market-Review.pdf.

107. Ортіна Г. Глобальні виклики та стратегічні аспекти інформаційної безпеки. Державна політика і управління в галузі освіти: зміст та сучасні виклики. С. 318-321.

108. Панасюк Т. І., Петренко С.В. Сучасний стан державно-приватного партнерства у сфері кібербезпеки: досвід України. Інформаційна безпека людини, суспільства, держави. 2025. № 1. С. 42-51.

109. Паршина О. А., Паршин Ю.І Кібербезпека в сучасних умовах зростання загроз національній та світовій безпеці. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2024. № 1. С. 36-44.

110. Петрик В., Присяжнюк М., Мельник Д. Кібербезпека держави. К.: ДНУ «Книжкова палата України». 2016. С. 10.

111. Поліщук В. Аналіз технології блокчейн у сфері кібербезпеки та захисту інформації. 2023. URL: https://openarchive.nure.ua/items/388e8be9-5443-46e2-bcd1-a381751127e4.

112. Поляков О. М. Особливості залучення приватного сектору до здійснення заходів у сфері забезпечення кібербезпеки, стримування деструктивної діяльності у кіберпросторі: кращі практики європейського досвіду. Інформація і право. 2025. № 3. С. 157-168.

113. Попова Д., Яременко С. Кібербезпека в епоху індустрії 5.0: нові виклики та можливості. Економічний вісник Донбасу. №3 (77). 2024. URL: https://doi.org/10.12958/1817-3772-2024-3(77)-203-216.

114. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23.02.2006 № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15#Text.

115. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.

116. Про затвердження Загальних вимог з кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від

19.06.2019 № 518. URL: https://zakon.rada.gov.ua/laws/show/518-2019-%D0%BF#Text.

117. Про затвердження Мінімальних вимог до захисту інформаційних, електронних комунікаційних, інформаційно-комунікаційних та технологічних систем: Постанова Кабінету Міністрів України від 29.03.2006 № 373. URL: https://zakon.rada.gov.ua/laws/show/373-2006-%D0%BF#Text.

118. Про затвердження Положення про організаційно-технічну модель кіберзахисту: Постанова Кабінету Міністрів України; Положення від 29.12.2021 № 1426. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text.

119. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та електронних комунікаційних [...]: Постанова Кабінету Міністрів України від 16.11.2002 № 1772. URL: https://zakon.rada.gov.ua/laws/show/ 1772-2002-%D0%BF#Text.

120. Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій [...]: Наказ Адміністрації Держспецзв'язку від 10.06.2008 № 94. URL: https://zakon.rada.gov.ua/laws/show/z0603-08#Text.

121. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних [...]: Наказ Адміністрації Держспецзв'язку від 02.12.2014 № 660. URL: https://zakon.rada.gov.ua/laws/ show/z0090-15#Text.

122. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених у мережі Інтернет: Адміністрація Держспецзв'язку; Наказ, Порядок, Акт [...] від 15.01.2016 № 20. URL: https://zakon.rada.gov.ua/laws/show/z0196-16#Text.

123. Про затвердження Правил надання та отримання електронних комунікаційних послуг: Постанова Кабінету Міністрів України від 25.06.2025 № 761. URL: https://zakon.rada.gov.ua/laws/show/761-2025-%D0%BF#Text.

124. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

125. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text.

126. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

127. Про об'єкти критичної інфраструктури та їх захист. Проект Закону України від 17.03.2021 № 5219-1. URL: https://ips.ligazakon.net/document/JI04668A.

128. Про оборону України: Закон України від 06.12.1991 № 1932-XII. URL: https://zakon.rada.gov.ua/laws/show/1932-12#Text.

129. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

130. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text.

131. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України; Стратегія від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

132. Пугачов О. Зарубіжний досвід забезпечення інформаційної безпеки держави. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2024. № 13. URL: https://reicst.com.ua/pmtl/article/view/2024-13-02-07/2024-13-02-07

133. Пузирний В. Ф., Захарчук І.В. Правові аспекти використання штучного інтелекту у сфері кібербезпеки: регулювання та етичні дилеми. Науковий вісник Сіверщини. Серія : Право. 2025. № 3. С. 58-69.

134. Пядишев В. Г. Кібербезпека критичних інфраструктур: закордонний досвід та українські реалії. Південноукраїнський правничий часопис. 2022. № 4(3). С. 229-234.

135. Радченко О. Захист критичної інформаційної інфраструктури: міжнародний досвід та українські реалії. Київ: Юрінком Інтер. 2020. с. 218.

136. Разумей Г.Ю., Разумей М.М. Діджиталізація публічного управління як складник цифрової трансформації України. Публічне управління та митне адміністрування, 2020. № 2 (25). С. 139-145.

137. Рекомендації та перспективи впровадження досвіду іноземних держав в систему формування генезису розвитку кібертехнологій у сфері безпеки та оборони України. Social Development and Security. 2023. Т. 13. № 4. С. 63-80.

138. Рогов П., Воровіч Б., Ткаченко В. Шляхи забезпечення кібернетичноїбезпеки об’єктів критичної інформаційної інфраструктури держави у воєнній сфері. Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняховського. 2017. 59(1). С. 64-72.

139. Рядінська В. Правове регулювання цифровізації публічного управління в Європейському Союзі. Академічні візії. 2025. № 39. С. 1-8.

140. Санжарова Г. Ф., Бак В.І., Санжаров В.А. Правові рамки кібербезпеки та політика захисту кіберпростору Республіки Польща. Науковий вісник Ужгородського національного університету. Серія : Право. 2025. Вип. 89(1). С. 163-168.

141. Семенченко А.І., Плескач В.Л., Заярний О.А., Плескач М.В. Організаційно-правові механізми державного управління забезпеченням кібербезпеки та кіберзахисту України: сутність, стан та перспективи розвитку. Проблеми програмування. 2020. № 2-3. С. 278-286.

142. Сиротін В. Д. Особливості цифровізації у сфері публічного управління. Проблеми сучасних трансформацій. Серія: право, публічне

управління та адміністрування. 2023. № 9. С. 1-4. DOI: https://doi.org/10.54929/2786-5746-2023-9-02-06.

143. Скіцько О. І., Ширшов Р.А. Нормативно-правове забезпечення кібербезпеки об'єктів критичної інфраструктури. Науковий вісник Львівського державного університету внутрішніх справ. серія юридична. 2024. Вип. 2. С. 73-79.

144. Служба безпеки України. Офіційний сайт. URL: https://ssu.gov.ua.

145. Станіславський Т. В. Стан та удосконалення механізму державного управління виконанням стратегії кібербезпеки України. Економіка та держава. Серія: Державне управління. 2019. №4. С. 1-5.

146. Стельмах А. Сучасні аспекти розвитку цифровізації у системі національної безпеки: закордонний досвід. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2025. №12. С. 141-147.

147. Студзінський Р. Теоретичні основи публічного управління у сфері забезпечення кібербезпеки України. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. 2025. №18. URL: https://reicst.com.ua/pmtl/article/view/2025-18-02-03/2025-18-02-03.

148. Тарасюк А. В. Теоретико-правове підґрунтя інформаційної етики в системі забезпечення кібербезпеки. Правова позиція. 2020. № 4. С. 48-52.

149. Ткаченко О., Ткаченко К. Кіберпростір і кібербезпека: проблеми, перспективи, технології. Цифрова платформа: інформаційні технології в соціокультурній сфері. Вип. 1. 2018. С. 75-86.

150. Топчій В. Проблемні питання забезпечення кібербезпеки в Україні. Аналітично-порівняльне правознавство. 2025. № 1. С. 664-669.

151. Третяк Ю. Система суб'єктів адміністративно-правового забезпечення кібербезпеки. Вісник Національного університету «Львівська політехніка». Серія : Юридичні науки. 2024. Т. 11, № 2. С. 197-205.

152. Труш О., Василенко Д. Забезпечення кібербезпеки при прийнятті рішень органами публічного управління. Державне будівництво. 2019. №2. URL: https://periodicals.karazin.ua/db/article/download/19261/17544.

153. Український ринок кібербезпеки зріс у чотири рази за вісім років. URL: https://aspeninstitutekyiv.org/ukrainskyi-rynok-kiberbezpeky-zris-u-chotyry-razy-za-visim-rokiv.

154. Управління ризиками кібербезпеки: основи та найкращі практики. URL: https://visuresolutions.com/uk/alm-guide/%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96% D0%BD%D0%BD%D1%8F-%D1%80%D0%B8%D0%B7%D0%B8%D0%BA %D0%B0%D0%BC%D0%B8-%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B8.

155. Федик В. Р., Денисенко Г. В. Теоретико-методологічні підходи до управління ризиками кібербезпеки на об’єктах критичної інфраструктури: реагування на кіберінциденти та менеджмент кризових ситуацій. Інформація і право, 2024. Вип. 1 С. 195-202.

156. Федорченко О. С. Роль штучного інтелекту у забезпеченні кібербезпеки України: сучасний стан та перспективи розвитку. Інформація і право. 2025. № 3. С. 139-146.

157. Федорченко О. С. Удосконалення координації діяльності суб’єктів забезпечення національної системи кібербезпеки. Нове українське право. 2024. Вип. 5. С. 71-77.

158. Худинцев М. М., Палажченко І.Л. Моделі зрілості кібербезпеки для оцінювання кібербезпеки у критичній інфраструктурі. Екологічна безпека та природокористування. 2024. Вип. 4. С. 122-134.

159. Худолій Ю. Проблеми і перспективи забезпечення кібербезпеки в умовах воєнного стану. Сталий розвиток: виклики та загрози в умовах сучасних реалій : матеріали II Міжнародної наук.–практ. Інтернет–конф., 06 черв. 2024 р. Полтава : Нац. ун–т ім. Юрія Кондратюка. 2024. С. 172-174.

160. Хусаінов П. В., Штаненко С.С. Обгрунтування інформаційної підтримки фахівця з реагування на інциденти кібербезпеки об’єкта критичної інфраструктури. Системи і технології зв'язку, інформатизації та кібербезпеки. 2025. № 8. С. 269-279.

161. Цифровізація: переваги та шляхи подолання викликів. Разумков центр. URL: https://razumkov.org.ua/statti/tsyfrovizatsiia-perevagy-ta-shliakhy-podolannia-vyklykiv.

162. Цюприк І. В. Публічно-приватне партнерство як стратегічний інструмент забезпечення кібербезпеки в умовах правового режиму воєнного стану в Україні. Міжнародний науковий журнал «Інтернаука». Серія : Юридичні науки. 2025. № 6. С. 46-52.

163. Чаплінська Ю. Кіберкультура та кібербезпека в умовах війни: психологічний практикум: практичний посібник. Національна академія педагогічних наук України, Інститут соціальної та політичної психології. Київ. 2023. с. 15-19.

164. Червяков О. Особливості забезпечення кібербезпеки як провідної складової національної безпеки України. Вісник кримінологічної асоціації України. 2024. №3 (33). URL: https://doi.org/10.32631/vca.2024.3.47.

165. Шайхет С. Механізми реалізації сервісно-орієнтовної державної політики у сфері інформаційної безпеки України: дис….канд. наук з держ. упр. 25.00.02 / НАДУ. Київ, 2019. С. 112, 113.

166. Шемчук В. Зарубіжний досвід забезпечення інформаційної безпеки держави. Порівняльно-аналітичне право. 2019. № 2. С. 189.

167. Щодо кібератак на сайти державних органів. Офіційний веб-сайт Державної служби спеціального зв'язку та захисту інформації України. URL: https://cip.gov.ua/ua/news/shodo-kiberatak-na-saiti-der- zhavnikh-organiv.

168. Щодо кібератаки на сайти військових структур та державних банків. Офіційний веб-сайт Кабінету Міністрів України. URL: https://www.kmu.gov.ua/news/shchodo-kiberataki-na-sajti-vijskovih-struktur-ta-derzhavnih-bankiv.

169. AlDaajeh S., Saleous H., Alrabaee S., Barka E., Breitinger F., Choo K.K.R. The Role of National Cybersecurity Strategies on the Improvement of Cybersecurity Education. Computers and Security. 2022. P. 119. URL: https://doi.org/10.1016/j.cose.2022.102754.

170. American Chamber of Commerce in Ukraine. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. BDO Global. 05.02.2024. URL: https://chamber.ua/ua/news/rol-shtuchnoho-intelektu-v-kiberbezpetsi-peredbachennia-ta-zapobihannia-atakam.

171. An official website of the European Union. URL: https://europa.eu/ european-u.

172. Angelini M., Ciccotelli C., Franchina L., Marchetti-Spaccamela A., Querzoni L. Italian National Framework for Cybersecurity and Data Protection. In Privacy Technologies and Policy. Springer: Cham. Switzerland. 2020. C. 134.

173. Australian Signals Directorate (ASD). URL: https://www.asd.gov.au

174. Brzostek A. Germany's Cybersecurity Policy. Teka Komisji Prawniczej PAN Oddział w Lublinie. 2022. Vol. 15 (2). PP. 61-72.

175. Case study e-Estonia: digital society & open data. URL: https://urbact.eu/sites/default/files/2024-07/E-Estonia%20Case%20Study.pdf.

176. Christakis T. European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence/ Grenoble Alpes Data Institute. 2020. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098.

177. Craigen D., Diakun-Thibault N., Purse R. Defining Cybersecurity. Technology Innovation Management Review. October 2014. P.13-21.

178. Crespi F., Caravellla S., Menghini M., Salvatori Ch. European Technological Sovereignty: An Emerging Framework for Policy Strategy. Intereconomics. Review of European Economic Policy. 2021. Vol. 56(6). P. 348-354/

179. Cyber Diplomacy: A New Frontier in International Relations and Professional Practice. EDRM. 2024. URL: https://edrm.net/2024/ 06/cyber-diplomacy-anew-frontier-in-international-relations-and-professional-practice.

180. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov.

181. Del-Real C., Díaz-Fernández A. M. Understanding the plural landscape of cybersecurity governance in Spain: A matter of capital exchange. International Cybersecurity Law Review. 2022. Vol. 3 (2). PP. 313-343.

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

183. European cebercrime centre. An official website of the European Union Agency for Law Enforcement Cooperation. URL: https://www.europol. europa.eu/ about-europol/european-cybercrime-centre-ec3.

184. Ganapati S., Ahn M., Reddick C. Evolutionof Cyber security Concerns: A Systematic Literature Review. In: 24th Annual International Conferenceon Digital Government Research (DGO) – Together in the Unstable World – Digital Governmentand Solidarity. Gdansk. 11–14 July. 2023. P. 90.

185. Goodall A. Cyber Security: Law and Practice. Sweet & Maxwell. 2020.

186. Information Security Risk Assessment / I. Kuzminykh, B. Ghita, V. Sokolov, T. Bakhshi. MDPI Encyclopedia. 2021. № 1. P. 602-617.

187. Jacuch A. Comparative Analysis of Cybersecurity Strategies. European Union Strategy and Policies. Polish and Selected Countries Strategies. Online Journal Modelling the New Europe. 2021. C. 110

188. Kaponig H. Austria's National Cyber Security and Defense Policy. Connections. 2020. Vol. 19 (1). P. 25.

189. Kozubtsova L. Performance indicators of the functioning of the information security system and cybersecurity of critical information infrastructure objects. Computer-integrated technologies: education, science, production. 2022. №48. P. 64-69. URL: https://doi.org/10.36910/6775-2524-0560-2022-48-10.

190. Kranenbarg, M. W., Leukfeldt, R. Artificial Intelligence and Cybersecurity: The Impact on Legal and Ethical Issues. Springer. 2021.

191. Kubanov V. Teoretychni pidkhody do poniatiino-katehorialnoho aparatu kiberbezpeky v systemi publichnoho upravlinnia. Aspekty publichnoho upravlinnia. 2018. №6 (8). P. 52. URL: https://doi.org/10.15421/151846.

192. Limba T., Pleta T., Agafonov K., Damkus M. Cyber security management model for critical in frastructure. Entre preneurshipand Sustainability Issues. 2017. № 4 (4). P. 559.

193. Magistretti S., Dell'Era C., Petruzzelli A. M. How Intelligentis Watson? Enabling Digital Transformation through Artificial Intelligenc. Business Horizons. 2019. Vol. 62. N 6. P. 819-829.

194. Milov O., Milevskyi S., Korol O. Developing an advanced classifier of threat for security agent behavior models. Наука і техніка Повітряних Сил Збройних Сил України. 2019. № 4 (37). P. 107.

195. National Cyber Security Index – NCSI. URL: https://ncsi.ega.ee/ncsi-index.

196. National Initiative for Cybersecurity Careers and Studies. Explore Terms: A Glossary of Common Cybersecurity Words and Phrases. URL: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c.

197. National Institute of Standards and Technology U.S. Report. Managing Information Security Risk: Organization Mission and Information System View.

198. Savchenko, O. S. Suchasni tendentsii zaprovadzhennia tsyfrovizatsii publichnoho upravlinnia v krainakh Yevropeiskoho Soiuzu. Publichne upravlinnia ta mytne administruvannia, Spetsvypusk, Special issue, 2022. PP. 117-122. DOI: https://doi.org/10.32782/2310-9653-2022-spec.19.

199. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. URL: https://ccdcoe.org/library/publications/ the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisa tional-analysis.

200. The National Cyber Security Centre(NCSC). URL: https://www.ncsc.gov.uk.

201. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. URL: https://ccdcoe.org.

202. Tvaronavičienė M., Plėta T., Della Casa S., & Latvys, J. Cyber security management of critical energy infrastructure in national cybersecurity strategies:

Cases of USA, UK, France, Estonia and Lithuania. Insights into regional development. 2020. 2 (4). С. 805.

203. Unit 8200: Israel's Information Warfare Unit. URL: https://greydynamics.com/unit-8200-israels-information-warfare-unit.

ДОДАТКИ

ДОДАТОК А

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Статті у наукових фахових виданнях України (одноосібні):

Студзінський Р. В. Роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні. *Інвестиції: практика та досвід.* № 22. 2025. С. 355-358.

DOI: 10.32702/2306-6814.2025.22.355

URL: https://www.nayka.com.ua/index.php/investplan/article/view/8085/8217

2. Студзінський Р. В. Теоретичні основи публічного управління у сфері забезпечення кібербезпеки України. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* № 18. 2025.

DOI: https://doi.org/10.54929/2786-5746-2025-18-02-03

URL: https://reicst.com.ua/pmtl/article/view/2025-18-02-03/2025-18-02-03

3. Студзінський Р. В. Зарубіжний досвід управління у сфері забезпечення кібербезпеки та його імплементація в Україні. *Наукові інновації та передові технології.* № 1 (53). 2026. С. 270-280.

DOI: https://doi.org/10.52058/2786-5274-2026-1(53)-270-281

URL: https://perspectives.pp.ua/index.php/nauka/article/view/35574

Тези конференцій

4. Студзінський Р. В. Необхідність забезпечення кібербезпеки України в сучасних умовах. Матеріали IX міжнародної науково-практичної конференції «Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України» (м. Київ, 11 листопада 2025 р.) С. 36-38.

5. Студзінський Р. В. Наукові підходи до визначення публічного управління у сфері забезпечення кібербезпеки України. Матеріали Міжнародної науково-практичної конференції «Наука, освіта, економіка та суспільство: адаптація до викликів 21 століття». (Сан-Франциско, США, 6 грудня 2025 р.). С. 156-158.

6. Студзінський Р.В. Європейський досвід публічного управління у сфері забезпечення кібербезпеки. Матеріали LXIII Міжнародної науковопрактичної конференції «Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку» (07 грудня 2025 р. м. Оломодць (Чехія). С. 60-62.

Додаток Б

Довідки про впровадження результатів дисертації

ЗАТВЕРДЖУЮ
Перший проректор (з навчальної роботи)
Національної академії СБ України
доктор технічних наук, доцент

Євген МЕЛЕНТІ

«30» 04 2026 року

АКТ
впровадження в освітній процес
Національної академії Служби безпеки України
результатів дисертаційного дослідження

«30» 04 2026 року м. Київ

Про впровадження в освітній процес Національної академії СБ України результатів дисертаційного дослідження Студзінського Романа Вікторовича на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України», поданого на здобуття ступеня доктора філософії за спеціальністю 281 – Публічне управління та адміністрування»

Комісія у складі:

голови: завідувача кафедри кібербезпеки центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України, доктора технічних наук, професора Вавіленкової А.І.

членів комісії: доцента кафедри кібербезпеки центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України, кандидата технічних наук, доцента Добришина Ю.Є.

заступника директора центру кібербезпеки - начальника наукової лабораторії протидії кіберзагрозам центру кібербезпеки Навчально-наукового інституту інформаційної безпеки та стратегічних комунікацій Національної академії СБ України, кандидата технічних наук, старшого наукового співробітника Скіцька О.І.

склала цей акт з приводу того, що результати дисертаційного дослідження здобувача ступеня доктора філософії Студзінського Романа Вікторовича на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України», зокрема, результати проведення SWOT-аналізу ефективності реалізації механізмів публічного управління у сфері забезпечення кібербезпеки України та схема комплексного механізму удосконалення публічного управління у сфері забезпечення кібербезпеки України використовується під час викладання навчальної дисципліни «Управління кіберінцидентами» освітньо-професійної програми «Кіберзахист у сфері інформаційних технологій та кіберпросторі» спеціальності К3 «Національна безпека».

Враховуючи викладене, комісія підтверджує, що результати дисертаційного дослідження Студзінського Р. В. мають теоретичне та практичне значення і використовуються в освітньому процесі Національної академії СБ України.

Голова комісії:
Доктор технічних наук,
професор
«20» 04 2026 року — Анастасія ВАВІЛЕНКОВА

Члени комісії:
кандидат технічних наук,
доцент
«20» 04 2026 року — Юрій ДОБРИШИН

кандидат технічних наук,
старший науковий співробітник
«20» 04 2026 року — Олексій СКІЦЬКО

ЗАТВЕРДЖУЮ
Начальник ІСЗЗІ КПІ ім. Ігоря Сікорського
бригадний генерал Олександр ПУЧКОВ
19.03.2026

АКТ
впровадження результатів дисертаційного дослідження
Студзінського Романа Вікторовича
в освітньому процесі

Комісія у складі голови комісії, заступника начальника Інституту (з навчальної роботи) кандидата технічних наук, доцента полковника Гиренка Ігоря Миколайовича, та членів комісії, заступника завідувача Спеціальної кафедри № 5 доктора філософії полковника Микитюка Артема В'ячеславовича, доцента Спеціальної кафедри № 5 кандидата технічних наук, доцента полковника Цуркана Василя Васильовича, цим Актом засвідчує впровадження результатів дисертаційного дослідження Студзінського Романа Вікторовича в освітньому процесі Інституту спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського" при підготовці фахівців на другому (магістерському) рівні вищої освіти за спеціальністю F3 Комп'ютерні науки. Зокрема, використано комплекс інноваційних інструментів кіберзахисту на об'єктах критичної інфраструктури під час проведення занять з освітнього компонента "Інформаційні технології в національній системі кібербезпеки".

Ефект від такого впровадження полягає в тому, що завдяки використанню удосконаленого комплексу інноваційних інструментів кіберзахисту на об'єктах критичної інфраструктури здобувачі вищої освіти краще усвідомлюють процес впровадження сучасних технологічних рішень, зокрема систем моніторингу кіберінцидентів, управління інформаційною безпекою, реагування на кібератаки та відновлення функціонування критично важливих систем.

Голова комісії:
Заступник начальника Інституту
(з навчальної роботи)
кандидат технічних наук
полковник Ігор ГИРЕНКО

Члени комісії:
Заступник завідувача Спеціальної кафедри № 5
доктор філософії
полковник Артем МИКИТЮК

Доцент Спеціальної кафедри № 5
кандидат технічних наук, доцент
полковник Василь ЦУРКАН

05/08-4а
12.03.2026

ЗАТВЕРДЖУЮ
Проректор
Національної академії
внутрішніх справ,
доктор юридичних наук, професор
полковник поліції
Олег ТАРАСЕНКО
10 квітня 2026 року

АКТ

10.04.2026 м. Київ № 91-49

Впровадження результатів дисертації Студзінського Р.В. на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України» у наукову діяльність НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи в складі:

– т.в.о. начальника відділу організації наукової діяльності, кандидата філософських наук, старшого дослідника майора поліції Антіпової Ольги Петрівни;

– завідувача кафедри адміністративного права та процесу, доктора юридичних наук, професора полковника поліції Доценка Олександра Сергійовича;

– т.в.о. завідувача науково-дослідної лабораторії з проблем державотворення та правозастосування ННІПП, кандидата юридичних наук, доцента Старицької Ольги Олексіївни;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й проаналізувала наукові праці Студзінського Р.В. на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України».

Проаналізовано основні результати дослідження Студзінського Р.В., зокрема наукові праці, у яких опубліковані теоретичні положення дисертації, а саме:

1. Студзінський Р. В. Роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні. *Інвестиції: практика та досвід.* № 22. 2025. С. 355–358. URL: https://www.nayka.com.ua/index.php/investplan/article/view/8085/8217.

2. Студзінський Р. В. Теоретичні основи публічного управління у сфері забезпечення кібербезпеки України. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* № 18. 2025. URL: https://reicst.com.ua/pmtl/article/view/2025-18-02-03/2025-18-02-03

3. Студзінський Р. В. Зарубіжний досвід управління у сфері забезпечення кібербезпеки та його імплементація в Україні. *Наукові інновації та передові технології.* № 1 (53). С. 270–280

4. Студзінський Р. В. Необхідність забезпечення кібербезпеки України в сучасних умовах. *Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України* : матеріали IX Міжнар. наук.-практ. конф. (Київ, 11 листоп. 2025 р.). С. 36–38.

5. Студзінський Р. В. Наукові підходи до визначення публічного управління у сфері забезпечення кібербезпеки України. *Наука, освіта, економіка та суспільство: адаптація до викликів 21 століття* : матеріали LXIII Міжнар. наук.-практ. конф. (Сан-Франциско, США, 6 груд. 2025 р.). С. 156–158.

6. Студзінський Р. В. Європейський досвід публічного управління у сфері забезпечення кібербезпеки. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* : матеріали LXIII Міжнар. наук.-практ. конф. (Оломодць (Чехія), 7 груд. 2025 р.). С. 60–62.

На основі проведеного аналізу комісія дійшла висновку про те, що зазначені вище наукові праці Студзінського Романа Вікторовича, мають високий теоретичний рівень та практичну значущість і можуть бути використані під час підготовки монографій, підручників, навчальних посібників, методичних рекомендацій, узагальнення аналітичних матеріалів, обґрунтування пропозицій до чинних проєктів нормативно-правових актів, підготовка яких потребує проведення відповідних наукових досліджень або містить наукову складову.

Члени комісії: **Ольга АНТІПОВА**

Олександр ДОЦЕНКО

Ольга СТАРИЦЬКА

Олена ТИХОНОВА

Людмила ГАЙДАР

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ,
доктор юридичних наук, професор
полковник поліції
Сергій ЧЕРНЯВСЬКИЙ
2026 року

АКТ

10.04.2026 м. Київ № 90-ОП

Впровадження результатів дисертації Студзінського Р.В. на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України» в освітній процес НАВС

Уклала експертна комісія з виявлення, узагальнення та впровадження позитивного досвіду роботи у складі:

– начальника відділу організації освітнього процесу старшого лейтенанта поліції Бойчук Вікторії Олександрівни;

– т.в.о. начальника відділу організації наукової діяльності, кандидата філософських наук, старшого дослідника майора поліції Антіпової Ольги Петрівни;

– завідувача кафедри адміністративного права та процесу, доктора юридичних наук, професора полковника поліції Доценка Олександра Сергійовича;

– завідувача кафедри кримінології та інформаційних технологій, доктора філософії капітана поліції Школьнікова Владислава Ігоровича;

– начальника відділу аспірантури (ад'юнктури) і докторантури, доктора юридичних наук, професора підполковника поліції Тихонової Олени Вікторівни;

– завідувача загальної бібліотеки Гайдар Людмили Георгіївни.

Комісія розглянула й проаналізувала наукові праці Студзінського Р.В. на тему «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України».

Проаналізовано основні результати дослідження Студзінського Р.В., зокрема наукові праці, у яких опубліковані теоретичні положення дисертації, а саме:

1. Студзінський Р. В. Роль державно-приватного партнерства у забезпеченні кібербезпеки в Україні. *Інвестиції: практика та досвід*. № 22. 2025. С. 355–358. URL: https://www.nayka.com.ua/index.php/investplan/article/view/8085/8217.

2. Студзінський Р. В. Теоретичні основи публічного управління у сфері забезпечення кібербезпеки України. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. № 18. 2025. URL: https://reicst.com.ua/pmtl/article/view/2025-18-02-03/2025-18-02-03

3. Студзінський Р. В. Зарубіжний досвід управління у сфері забезпечення кібербезпеки та його імплементація в Україні. *Наукові інновації та передові технології.* № 1 (53). С. 270–280

4. Студзінський Р. В. Необхідність забезпечення кібербезпеки України в сучасних умовах. *Теоретико-практичні засади управління, економіки та природокористування: аспекти реінтеграції Криму в господарський комплекс України* : матеріали IX Міжнар. наук.-практ. конф. (Київ, 11 листоп. 2025 р.). С. 36–38.

5. Студзінський Р. В. Наукові підходи до визначення публічного управління у сфері забезпечення кібербезпеки України. *Наука, освіта, економіка та суспільство: адаптація до викликів 21 століття* : матеріали LXIII Міжнар. наук.-практ. конф. (Сан-Франциско, США, 6 груд. 2025 р.). С. 156–158.

6. Студзінський Р. В. Європейський досвід публічного управління у сфері забезпечення кібербезпеки. *Сучасні аспекти модернізації науки: стан, проблеми, тенденції розвитку* : матеріали LXIII Міжнар. наук.-практ. конф. (Оломодць (Чехія), 7 груд. 2025 р.). С. 60–62.

На основі проведеного аналізу комісія зробила висновок, що наукові праці Студзінського Романа Вікторовича, містять науково обґрунтовані теоретичні положення і практичні рекомендації, що дає підстави запровадити їх для використання в освітньому процесі Національної академії внутрішніх справ, зокрема під час викладання навчальних дисциплін «Адміністративне право», «Технології прийняття управлінських рішень», «Управління в правоохоронних органах», «Управлінський контроль в публічній сфері», «Прийняття ефективних рішень», «Інформаційні системи та технології в публічному управлінні», «Інформаційно-аналітичне забезпечення правоохоронної діяльності», підготовки навчально-методичних і дидактичних матеріалів, а також рекомендувати їх до вивчення під час самостійної роботи здобувачів вищої освіти.

Члени комісії: **Вікторія БОЙЧУК**

Ольга АНТІПОВА

Олександр ДОЦЕНКО

Владислав ШКОЛЬНІКОВ

Олена ТИХОНОВА

Людмила ГАЙДАР

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТАВРІЙСЬКИЙ НАЦІОНАЛЬНИЙ
УНІВЕРСИТЕТ ІМЕНІ В. І. ВЕРНАДСЬКОГО
V. I. VERNADSKY TAURIDA NATIONAL UNIVERSITY
вул. Дж. Маккейна, 33, м. Київ, 01135, тел. (044) 529 05-16
e-mail: crimea.tnu@gmail.com код ЄДРПОУ 02070967

13.01.2026 № 18

на № _____ від_____

ДОВІДКА
про впровадження у навчальний процес
результатів дисертаційного дослідження
Студзінського Романа Вікторовича за темою
«Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України»

Результати дисертаційного дослідження Студзінського Романа Вікторовича за темою «Розвиток механізмів публічного управління у сфері забезпечення кібербезпеки України» враховано та частково використано при формуванні змісту дисципліни «Глобалізація управління суспільними процесами, євроінтеграція та безпека» освітнього рівня магістра за спеціальністю 281 «Публічне управління та адміністрування». Для розвитку знань та управлінських навичок студентів використано теоретичні положення дисертаційного дослідження та пропозиції Студзінського Романа Вікторовича щодо інноваційних інструментів кіберзахисту на об'єктах критичної інфраструктури.

Проректор
з науково-педагогічної діяльності
та інноваційного розвитку **Олександр БЕССАРАБ**

Директор Навчально-наукового
інституту управління, економіки
та природокористування **Володимир ГОРНИК**