МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ПОЛІСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет права, публічного управління
та національної безпеки
Кафедра економічної теорії,
інтелектуальної власності
та публічного управління

Кваліфікаційна робота
на правах рукопису

НОМЕРЧУК ІВАН РУСЛАНОВИЧ
(прізвище, ім'я, по батькові здобувача вищої освіти)

УДК 336:338
(індекс)

КВАЛІФІКАЦІЙНА РОБОТА
ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ ДЕРЖАВНОЇ ПОЛІТИКИ В СФЕРІ КІБЕРБЕЗПЕКИ

(тема роботи)

281 «Публічне управління та адміністрування»
(шифр і назва спеціальності)

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

І. Р. НОМЕРЧУК
(підпис, ініціали та прізвище здобувача вищої освіти)

Керівник роботи
ДАНКЕВИЧ Євген Михайлович
(прізвище, ім'я, по батькові)
доктор економічних наук, професор
(науковий ступінь, вчене звання)

Житомир – 2025

Висновок кафедри економічної теорії, інтелектуальної власності та публічного управління
за результатами попереднього захисту: **НОМЕРЧУКА Івана Руслановича** допущений до захисту

Протокол засідання кафедри економічної теорії, інтелектуальної власності та публічного управління № ____ від «____»_____ 2025 р.

Завідувач кафедри економічної теорії, інтелектуальної власності та публічного управління
к.е.н., професор _____ Валентина ЯКОБЧУК
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

«___» _____ 2025 р.

Результати захисту кваліфікаційної роботи

Здобувач вищої освіти **НОМЕРЧУК Іван Русланович** захистив
(прізвище ,ім'я, по батькові)

кваліфікаційну роботу з оцінкою:
сума балів за 100–бальною шкалою _____
за національною шкалою _____

Секретар ЕК
_____–_____ _____ Анастасія ПРУТ
(науковий ступінь, вчене звання) (підпис) (власне ім'я, прізвище)

АНОТАЦІЯ

НОМЕРЧУК І. Р. Формування та реалізація державної політики в сфері кібербезпеки.– Кваліфікаційна робота на правах рукопису. Кваліфікаційна робота на здобуття освітнього ступеня бакалавра за спеціальністю 281 «Публічне управління та адміністрування» – Поліський національний університет, Житомир, 2025.

У кваліфікаційній роботі досліджено особливості реалізації державної політики у сфері кібербезпеки в Україні в умовах цифрової трансформації та гібридної агресії. Проаналізовано міжнародний та національний досвід, нормативно-правову базу, роль основних суб'єктів кіберзахисту, а також інституційні та технологічні виклики. Обґрунтовано необхідність модернізації підходів до управління кіберзагрозами, впровадження принципів розвитку хмарної інфраструктури та цифрової грамотності. Результати дослідження можуть бути використані для вдосконалення публічної політики у сфері інформаційної безпеки.

Ключові слова: кібербезпека, цифрове урядування, публічне управління, інформаційна безпека, критична інфраструктура.

SUMMARY

NOMERCHUK I. Formation and implementation of state policy in the field of cybersecurity. Qualification work on manuscript rights. Qualification work for a bachelor's degree in specialty 281 «Public management and administration» – Polissia National University, Zhytomyr, 2025.

The qualification paper explores the specifics of implementing public policy in the field of cybersecurity in Ukraine amid digital transformation and hybrid aggression. It analyzes both international and national experience, the legal framework, the role of key cybersecurity actors, as well as institutional and technological challenges. The study substantiates the need to modernize approaches to cyber threat management, develop cloud infrastructure, and enhance digital literacy. The research results can be used to improve public policy in the sphere of information security.

Keywords: cybersecurity, digital governance, public administration, information security, critical infrastructure.

ЗМІСТ

ВСТУП

Актуальність теми дослідження. У сучасному світі кіберпростір став невід'ємною складовою життєдіяльності суспільства, держави та бізнесу. З розвитком цифрових технологій зросла і кількість загроз, пов'язаних із використанням інформаційно-комунікаційних систем. Зокрема, кібератаки стали інструментом гібридної війни, втручання у вибори, порушення роботи критичної інфраструктури. Україна, яка з 2014 року перебуває в умовах триваючої збройної агресії, стала однією з перших країн, що системно стикається з масштабними кіберзагрозами. Це обумовлює надзвичайну актуальність дослідження державної політики у сфері кібербезпеки, її нормативно-правового, інституційного та стратегічного забезпечення.

Метою дослідження є визначення теоретичних основ, аналіз поточного стану та розробка практичних пропозицій щодо вдосконалення державної політики кібербезпеки України в умовах цифрової трансформації та зовнішніх загроз.

Зазначена мета дослідження передбачає вирішення наступних завдань:

- проаналізувати поняття та принципи кібербезпеки в системі публічного управління;
- дослідити міжнародний досвід формування політики кібербезпеки (на прикладі ЄС, США, НАТО);
- охарактеризувати стан нормативно-правової та інституційної бази забезпечення кібербезпеки в Україні;
- виявити трансформації державної політики кібербезпеки у період воєнного стану;
- обґрунтувати шляхи модернізації законодавства та інтеграції цифрових інструментів для підвищення кіберстійкості.

Об'єктом дослідження є державна політика у сфері кібербезпеки.

Предмет дослідження: механізми формування та реалізації політики кібербезпеки в Україні в умовах сучасних викликів.

Методи дослідження. У роботі застосовано комплекс загальнонаукових і спеціальних методів: логіко-аналітичний метод для вивчення теоретичних основ кібербезпеки; системний підхід для аналізу інституційного механізму реалізації політики; порівняльно-правовий метод – для дослідження міжнародного досвіду; емпіричні методи – для виявлення проблем реалізації політики в Україні; метод структурно-функціонального аналізу – для формування практичних рекомендацій.

Перелік публікацій автора за темою дослідження. За темою дослідження опубліковано дві тези в збірниках науково-практичних конференцій Поліського національного університету.

Практичне значення отриманих результатів полягає у формулюванні рекомендацій щодо удосконалення державної політики у сфері кібербезпеки, які можуть бути використані у діяльності державних органів, під час підготовки стратегічних документів, у розробці програм з цифрової трансформації та безпеки, а також у навчальному процесі з дисциплін публічного управління.

Структура та обсяг роботи. Випускна кваліфікаційна робота містить вступ, три розділи основної частини та висновки до них, висновки та пропозиції, список використаних джерел. Основний текст роботи викладено на 32 сторінках. Список використаних джерел включає 42 найменування.

РОЗДІЛ 1.
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ КІБЕРБЕЗПЕКИ

1.1. Поняття та основні принципи кібербезпеки в публічному управлінні

Кібербезпека в системі публічного управління – це сукупність заходів і механізмів, спрямованих на захист інформаційних ресурсів, інфраструктури та цифрових послуг держави від кіберзагроз. Фактично під кібербезпекою розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави під час використання кіберпростору. Такий стан забезпечує стабільне функціонування органів влади й суспільних інститутів у цифровому середовищі, збереження конфіденційності, цілісності і доступності інформації, а також своєчасне виявлення, попередження та нейтралізацію реальних і потенційних загроз національній безпеці у кіберпросторі. У сфері публічного управління кібербезпека стала невід'ємною складовою національної безпеки та ефективного державного управління, особливо в умовах цифровізації суспільства і зростання залежності від інформаційно-комунікаційних технологій [5].

Державна політика у сфері кібербезпеки ґрунтується на низці фундаментальних принципів. Перш за все, це принцип верховенства права і законності, що передбачає відповідність усіх дій у кіберпросторі вимогам закону та повагу до прав і свобод людини. Органи публічної влади повинні забезпечувати кібербезпеку, дотримуючись правових норм і демократичних цінностей, а діяльність спеціалізованих кіберпідрозділів має перебувати під цивільним контролем і здійснюватися прозоро та підзвітно суспільству.

Другий ключовий принцип – пріоритет національних інтересів і національної безпеки. Кібербезпека розглядається як засіб захисту суверенітету та критично важливої інфраструктури держави. Політика в цій сфері має

сприяти захисту державних інформаційних систем, енергетичних, транспортних, фінансових та інших критичних об’єктів від кібератак, що можуть завдати шкоди суспільству чи обороноздатності країни. Держава несе основну відповідальність за координацію зусиль у протидії кіберзагрозам та реагуванні на кібератаки, забезпечуючи при цьому необхідні ресурси і повноваження відповідним органам.

Важливим є принцип забезпечення відкритого, стійкого та безпечного кіберпростору. Це означає, що держава, реалізуючи заходи кіберзахисту, одночасно підтримує розвиток глобальної мережі Інтернет, свободу онлайн-доступу та обміну інформацією. Забезпечення кібербезпеки не повинно призводити до надмірного обмеження прав громадян у цифровому середовищі; натомість акцент робиться на створенні умов для відповідальної поведінки в кіберпросторі та підвищенні загальної цифрової грамотності населення. Стійкість кіберпростору означає здатність систем витримувати та швидко відновлюватися після кібератак, що досягається шляхом впровадження найкращих практик кіберзахисту.

Наступний принцип – державно-приватне партнерство та взаємодія з суспільством. Успішна кібербезпекова політика неможлива без тісної співпраці державних органів із приватним сектором і громадянським суспільством. Більшість кіберінфраструктури і технологій належить саме приватним компаніям, тому обмін інформацією про кіберінциденти, спільні навчання, дослідницькі проекти та підготовка кадрів є необхідними елементами. Держава повинна стимулювати такі партнерства, створювати правові умови для обміну даними про загрози та інциденти, залучати експертне середовище й наукові установи до розробки ефективних рішень у сфері кіберзахисту.

Принцип пропорційності та адекватності заходів передбачає, що реагування на кіберзагрози має відповідати рівню реальних і потенційних ризиків. Держава застосовує такі засоби кіберзахисту, які є необхідними і достатніми для нейтралізації загрози, уникаючи як бездіяльності, так і надмірно жорстких кроків. Водночас визнається невід’ємне право держави на самозахист

у кіберпросторі у разі агресивних дій з боку зовнішніх суб'єктів. Іншими словами, якщо проти країни здійснюється масштабна кібератака, держава може вживати активних заходів захисту відповідно до національного законодавства та міжнародного права.

Невід'ємно з цим пов'язані принципи превентивності та невідворотності покарання. Пріоритет віддається саме попередженню кіберінцидентів: превентивні заходи, такі як моніторинг мереж, виявлення вразливостей, навчання персоналу, мають зменшити ймовірність успішних атак. Якщо ж правопорушення у кіберпросторі все-таки сталися, держава забезпечує невідворотність покарання для винних у кіберзлочинах. Це досягається через удосконалення законодавства, розвиток можливостей правоохоронних органів розслідувати кіберзлочини, міжнародну співпрацю у сфері екстрадиції кіберзлочинців тощо. Неуникність відповідальності виконує стримуючу функцію і підвищує довіру суспільства до державної політики у сфері безпеки.

Окремо варто підкреслити принцип розвитку власного науково-технічного потенціалу у сфері кібербезпеки. Державна політика заохочує створення та підтримку вітчизняних технологій кіберзахисту, розвиток інновацій, дослідницьких центрів і підготовки фахівців. Інвестиції у освіту та науку, формування професійних команд реагування на кіберінциденти і центрів моніторингу сприяють підвищенню спроможностей країни протистояти сучасним кіберзагрозам. Розвиток національної індустрії кібербезпеки також зміцнює економічну незалежність і забезпечує державу необхідними засобами захисту без критичної залежності від зовнішніх технологій.

І останнім вагомим принципом є міжнародне співробітництво. Кіберзагрози мають глобальний характер, тому жодна держава не може ефективно протидіяти їм ізольовано. Україна, як і інші країни, бере участь у міжнародних ініціативах, укладає угоди про обмін інформацією щодо кіберінцидентів, долучається до спільних навчань і тренувань, співпрацює в розслідуванні транскордонних кібератак. Міжнародна кооперація покликана зміцнити взаємну довіру між державами, виробити спільні стандарти і підходи

до кібербезпеки та не допустити використання кіберпростору для військових чи терористичних цілей [14].

Отже, поняття кібербезпеки в публічному управлінні охоплює широкий спектр питань – від захисту інформації до стратегічного реагування на кіберзагрози. Воно спирається на систему принципів, що забезпечують законність, національну безпеку, відкритість кіберпростору, співпрацю всіх зацікавлених сторін, адекватність заходів, невідворотність відповідальності, розвиток потенціалу та міжнародну взаємодію. Дотримання цих принципів є передумовою ефективного формування і реалізації державної політики у сфері кібербезпеки.

1.2. Міжнародні підходи до формування політики кібербезпеки: досвід ЄС, США, НАТО

Різні країни та міжнародні об’єднання виробили власні моделі кібербезпекової політики, які відображають їхні пріоритети та можливості. Досвід Європейського Союзу, США та НАТО є показовим у цьому контексті і слугує орієнтиром для інших держав, включно з Україною, у розбудові ефективної політики кібербезпеки.

Європейський Союз дотримується комплексного підходу до кібербезпеки, поєднуючи правове регулювання, інституційну координацію та стимулювання стійкості цифрового середовища. Ще у 2013 році було прийнято першу Стратегію кібербезпеки ЄС, яка визначила стратегічні цілі: підвищення кіберстійкості, зниження рівня кіберзлочинності, розбудова власних кіберзахисних можливостей, розвиток технологічної бази і формування узгодженої міжнародної політики у сфері кіберпростору [20]. В подальші роки ЄС створив розгалужену нормативно-правову базу: ухвалено директиву 2016/1148 про безпеку мережевих та інформаційних систем у 2016 році, яка зобов’язала країни-члени запровадити національні стратегії кібербезпеки,

визначити операторів критично важливих послуг і встановити вимоги до захисту їхніх мереж та систем [1]. У 2022 році було оновлено цю директиву; нова редакція, відома як NIS2, розширила перелік секторів і підприємств, на які поширюються вимоги з кібербезпеки, та посилила механізми обміну інформацією і координації між країнами ЄС [26].

Важливим елементом політики ЄС є функціонування спеціалізованих органів. Ключову роль відіграє Агентство ЄС з кібербезпеки, яке займається виробленням рекомендацій, аналізом кіберризиків, координацією між національними командами реагування на інциденти та проведенням кібернавчань. На рівні Євросоюзу створено також мережу компетентних центрів і груп швидкого реагування на кіберінциденти, що покращує готовність до спільного реагування на масштабні атаки. ЄС активно інвестує в підвищення кіберстійкості критичних інфраструктур: впроваджуються високі стандарти захищеності для енергетичних мереж, транспорту, фінансової сфери, охорони здоров'я та інших важливих секторів [24]. Особливу увагу приділено безпеці новітніх технологій, таких як мережі п'ятого покоління – розроблено вимоги та рекомендації для мінімізації ризиків, пов'язаних із ними.

Європейський Союз також розвиває так звану кібердипломатію – зовнішньополітичний вимір кібербезпеки. Встановлено механізми обміну інформацією про кіберінциденти між країнами-членами та партнерами, проводяться регулярні кібердіалоги з такими країнами, як США, Японія, Україна тощо [27]. ЄС сформував спільний підхід до відповідальної поведінки держав у кіберпросторі та запровадив санкційний режим проти іноземних осіб чи організацій, відповідальних за масштабні кібератаки на об'єкти в державах ЄС. Таким чином, підхід ЄС акцентує колективну безпеку: країни співпрацюють у межах союзних структур, дотримуються єдиних стандартів і разом реагують на спільні загрози.

Сполучені Штати Америки мають одну з найрозвиненіших систем кібербезпеки, яка спирається на потужний приватний сектор та значні державні інвестиції в оборону і розвідку. Державна політика США у сфері кібербезпеки

історично еволюціонувала під впливом як зростання кібератак, так і розвитку технологій. Ще у 2003 році була прийнята перша Національна стратегія кібербезпеки США, а в наступні роки регулярно оновлювалися стратегічні документи з урахуванням нових викликів. На національному рівні діє низка нормативних актів і структур: створено Агентство з кібербезпеки та безпеки інфраструктури (CISA) у складі Міністерства внутрішньої безпеки, яке координує захист федеральних мереж і критичної інфраструктури, ділиться попередженнями про загрози з приватними компаніями, розробляє стандарти кіберзахисту [25]. У США широко застосовується рамковий стандарт NIST Cybersecurity Framework, який рекомендує підприємствам і установам підходи для ефективного управління кіберризиками.

Американський підхід наголошує на партнерстві уряду та приватного сектору, оскільки більшість критичних об’єктів – енергетика, фінанси, транспорт, зв’язок – знаходяться в приватній власності. Уряд США стимулює обмін інформацією про кіберзагрози через створення галузевих центрів обміну та аналізу інформації, проводить регулярні спільні навчання з кібербезпеки за участю компаній і державних агентств. Значну увагу приділено захисту федеральних урядових мереж: запроваджено обов’язкові програми підвищення кіберстійкості відомств, перехід на концепцію нульової довіри у державних інформаційних системах, посилено вимоги до постачальників програмного забезпечення для уряду щодо безпеки їхніх продуктів [29].

Останніми роками США суттєво оновили свою кібербезпекову стратегію у відповідь на зростання масштабних атак, таких як атаки угруповань типу APT або інцидент із компанією SolarWinds, та геополітичні загрози з боку державних хакерських програм Росії і Китаю [43]. У 2023 році адміністрація США представила нову Національну стратегію кібербезпеки, яка передбачає два ключові зрушення: перше – перерозподіл відповідальності за кібербезпеку від кінцевих користувачів до розробників програмних продуктів і операторів систем (виробники програмного забезпечення та провайдери повинні нести більшу відповідальність за безпеку своїх продуктів); друге – проактивні дії

держави з нейтралізації кіберзагроз до того, як вони завдадуть шкоди [21]. Стратегія закликає запровадити жорсткіші регуляторні вимоги в різних галузях економіки щодо забезпечення кібербезпеки, посилити стандарти управління вразливостями, зокрема обов'язкове своєчасне встановлення оновлень та впровадження багатофакторної автентифікації, а також вимагати від хмарних сервісів верифікації іноземних клієнтів, аби ускладнити діяльність кіберзлочинців.

Одним із напрямів політики США є активне переслідування кіберзлочинців та хакерських угруповань: здійснюються як кримінальні заходи – висунення обвинувачень, екстрадиція правопорушників – так і кібероперації спецслужб, спрямовані на зрив діяльності ворожих хакерів чи знищення їхньої інфраструктури. США також ініціюють створення міжнародних коаліцій і домовленостей, щоби спільно з союзниками чинити тиск на держав-правопорушників у кіберпросторі, зокрема шляхом запровадження санкцій та інших дипломатичних заходів, та виробляти глобальні норми відповідальної поведінки [42].

У підході США простежується баланс між зміцненням внутрішньої кіберстійкості та демонстрацією сили на міжнародній арені. З одного боку, держава інвестує в кібербезпеку критичної інфраструктури, навчання кадрів, розвиток інновацій, зокрема підтримує стартапи у сфері кібербезпеки та впроваджує механізми кіберстрахування як спосіб управління ризиками. З іншого боку, США демонструють готовність застосувати свій кіберпотенціал у відповідь на атаки, а також очолюють глобальні ініціативи з кібербезпеки, співпрацюючи в рамках міжнародних форумів – ООН, Групи семи та двосторонніх союзів.

Організація Північноатлантичного договору розглядає кіберпростір як окремий домен безпеки поряд із сушею, морем, повітрям та космосом. Після серії кібератак на державні установи членів Альянсу, зокрема на Естонію у 2007 році [38], НАТО поступово вибудувало спільну політику кібероборони. У 2014 році на саміті в Уельсі союзники погодили посилену політику з

кіберзахисту, визнавши, що кібератака може становити загрозу настільки ж серйозну, як і збройний напад [37]. Було підтверджено, що у випадку надзвичайно руйнівної кібератаки на одну з країн-членів може бути задіяно статтю 5 НАТО про колективну оборону. У 2016 році на Варшавському саміті кіберпростір офіційно визнано оперативним доменом, що дозволило інтегрувати кіберзахист у військове планування та навчання нарівні з традиційними сферами [36].

Політика НАТО у сфері кібербезпеки фокусується на двох вимірах: захист власних мереж і систем Альянсу та допомога країнам-членам у підвищенні їх кіберстійкості. Для нарощування спроможностей союзників у сфері кіберзахисту під егідою НАТО створено Кооперативний центр передового досвіду з кібероборони (CCDCOE), розташований у місті Таллінн (Естонія), який займається дослідженнями, підготовкою кадрів та навчаннями у сфері кібербезпеки для країн НАТО. Створено також Координаційний центр реагування на комп'ютерні інциденти (NCIRC), який забезпечує цілодобовий моніторинг і захист інформаційних систем Організації, а у разі масштабного кіберінциденту може направляти групи швидкого реагування на допомогу постраждалій країні-члену [35]. НАТО розробило механізми обміну інформацією про кіберзагрози між союзниками, узгодило базові вимоги до кіберзахисту національних мереж оборони в рамках процесу оборонного планування Альянсу.

Підсумовуючи, міжнародні підходи до формування політики кібербезпеки в різних регіонах світу мають спільну мету – забезпечити стійкість цифрового простору та захист від кібератак, проте використовують різні інструменти й акценти. ЄС показує ефективність регуляторної та колективної моделі, США – інноваційної та проактивної, НАТО – оборонної коаліційної. Вивчення цього досвіду дозволяє окреслити найкращі практики й принципи, які можуть бути використані при формуванні та реалізації державної політики України у сфері кібербезпеки.

РОЗДІЛ 2.
СТАН І ПРОБЛЕМИ РЕАЛІЗАЦІЇ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ В УКРАЇНІ

2.1. Нормативно-правове забезпечення кібербезпеки в Україні

Нормативно-правове регулювання сфери кібербезпеки в Україні ґрунтується на положеннях Конституції України, законах України, зокрема тих, що визначають засади національної безпеки, внутрішньої і зовнішньої політики, а також регламентують захист державних інформаційних ресурсів та обробку інформації. До цього переліку також входять міжнародні договори, які ратифіковані Верховною Радою України, укази Президента України, нормативні акти Кабінету Міністрів України та інші підзаконні акти, ухвалені на виконання законів України.

Хоча Конституція України не містить безпосереднього терміна «кібербезпека», оскільки була прийнята до активного розвитку цифрових технологій і розширеного використання інтернету, в її положеннях закладено фундаментальні принципи, які можуть бути застосовані до цифрової безпеки. Так, стаття 31 Конституції гарантує право кожного на таємницю листування, телефонних розмов та інших форм зв’язку, що прямо стосується захисту комунікацій у кіберпросторі. Стаття 32 забороняє збирання, збереження, використання й поширення конфіденційної інформації про особу без її згоди, за винятком випадків, визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Ці положення Конституції мають безпосереднє відношення до захисту персональних даних і приватності в цифровому середовищі [4].

У межах забезпечення цифрової безпеки та протидії кіберзлочинності важливими є й положення Конституції, що стосуються функціонування системи правосуддя. Зокрема, статті 55–59 встановлюють засади справедливого судочинства, відповідальності перед законом і гарантії захисту прав громадян,

що мають бути реалізовані і в сфері кіберпростору, зокрема у випадках порушень прав унаслідок неправомірного доступу до інформації чи здійснення кібератак [4].

Одним із базових нормативно-правових актів, що заклав підвалини інформаційної політики незалежної України, є Закон України «Про інформацію» від 2 жовтня 1992 року № 2657-XII. Цей документ визначив основні принципи функціонування інформаційної сфери, забезпечив правові засади для регулювання обігу, зберігання, використання і захисту інформації, а також встановив засади державної інформаційної політики. Основні положення закону містять визначення поняття інформації та її видів, норми щодо доступу громадян до інформації, обов'язки та права суб'єктів інформаційних правовідносин, механізми правового захисту права на інформацію, а також правила щодо зберігання, обробки та охорони інформації, включно з відповідальністю за порушення встановлених норм [13].

Закон України «Про інформацію» відіграв важливу роль у формуванні фундаменту правового забезпечення інформаційного суспільства в Україні. Саме на його основі, у зв'язку з технологічним прогресом і трансформацією соціальних процесів, у подальшому було розроблено нові нормативно-правові акти, що регламентують захист інформації. Вперше на законодавчому рівні поняття інформаційної безпеки в Україні було закріплено в Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 9 січня 2007 року № 537-V. У цьому законі інформаційна безпека визначалась як стан захищеності життєво важливих інтересів людини, суспільства і держави, що забезпечується шляхом запобігання завданню шкоди внаслідок: неповноти, несвоєчасності або недостовірності інформації, яка використовується; деструктивного інформаційного впливу; негативних наслідків використання інформаційних технологій; несанкціонованого поширення, використання чи порушення цілісності, конфіденційності та доступності інформації [15].

Водночас у стандарті ISO/IEC 27032 поняття кібербезпеки подано крізь призму захисту кіберпростору, що трактується як забезпечення конфіденційності, цілісності та доступності інформації у цифровому середовищі. Згідно з цим стандартом, кіберпростір розуміється як середовище, сформоване в результаті функціонування на основі уніфікованих принципів і спільних правил інформаційних, телекомунікаційних та інформаційно-комунікаційних систем [32].

У свою чергу, відповідно до національного стандарту ДСТУ ISO/IEC 27032:2016, пункт 4.21, кіберпростір трактується як складне динамічне середовище, що виникає внаслідок взаємодії людей, програмного забезпечення та інтернет-сервісів через технічні пристрої або об’єднані мережі, яке не має фізично визначеного виміру [2].

На сьогодні одним із ключових нормативних актів, що регулює сферу кібербезпеки в Україні, є Закон України «Про основні засади забезпечення кібербезпеки України» № 2163-VIII, ухвалений 5 жовтня 2017 року. Цей закон визначає основні напрями та засади державної політики в галузі кібербезпеки, стратегічні завдання і механізми її реалізації, а також окреслює ключові принципи захисту інформації й інформаційних систем. Основна мета закону полягає у забезпеченні національної безпеки, захисті суверенітету, територіальної цілісності та національних інтересів України в кіберпросторі [14].

У змістовному плані закон визначає низку важливих складових. Зокрема, серед стратегічних завдань передбачається гарантування кібербезпеки об’єктів критичної інформаційної інфраструктури, державних інформаційних систем, а також інформаційних ресурсів, що мають суспільно важливе значення. У документі також наведено визначення базових термінів, які є ключовими для функціонування системи кібербезпеки, зокрема таких як кіберзагроза, кіберінцидент, кіберзлочин, кібероборона та інші.

У Законі закріплено перелік принципів, на яких ґрунтується національна політика у сфері кібербезпеки. До них належать: дотримання законності; повага

до прав і свобод людини; відкритість, доступність та стабільність кіберпростору; розвиток інфраструктури Інтернету; відповідальна поведінка суб'єктів у цифровому середовищі; забезпечення невідворотності відповідальності за кіберзлочини; прозорість дій суб'єктів забезпечення кібербезпеки; пріоритет національних інтересів України; міжнародне співробітництво з метою посилення довіри, координації зусиль у протидії кіберзагрозам і взаємодії у розслідуванні злочинів у кіберсфері. Особливу увагу приділено забороні використання кіберпростору в терористичних, військових або інших протиправних цілях.

Закон також передбачає створення та функціонування національної системи кібербезпеки, до складу якої входять такі ключові інституції, як Державна служба спеціального зв'язку та захисту інформації України, Міністерство оборони України, Генеральний штаб Збройних Сил України, Служба безпеки України, Національна поліція, розвідувальні органи, Національний банк України. Кожен із цих суб'єктів має чітко окреслені повноваження та обов'язки у сфері захисту кіберпростору, а також координує відповідні заходи згідно з покладеними функціями.

2.2. Інституційна структура управління кібербезпекою: функції державних органів (ДССЗЗІ, СБУ, РНБО тощо)

Забезпечення кібербезпеки є комплексним завданням, яке охоплює численні аспекти захисту національного інформаційного простору, критичної інформаційної інфраструктури та цифрового суверенітету держави. В Україні цю сферу курує розгалужена система інституцій, до складу якої входять як спеціалізовані органи, так і загальнодержавні структури безпекового та оборонного спрямування. Координація між цими суб'єктами, чіткий розподіл повноважень та відповідальності, а також дотримання єдиної стратегії є передумовами для побудови ефективної національної системи кіберзахисту.

Ключову роль у забезпеченні кібербезпеки відіграє Державна служба спеціального зв'язку та захисту інформації України. Вона є центральним органом виконавчої влади зі спеціальним статусом, відповідальним за реалізацію державної політики у сферах криптографічного та технічного захисту інформації, функціонування національної системи урядового зв'язку, а також розвитку і захисту критичної інформаційної інфраструктури. До її компетенції входить організація захисту державних інформаційних ресурсів, сертифікація технічних засобів захисту інформації, розробка та впровадження нормативних актів щодо інформаційної безпеки, проведення аудитів і перевірок захищеності інформаційних систем органів влади. Крім того, Держспецзв'язку координує діяльність національного центру реагування на комп'ютерні інциденти, що опікується виявленням, аналізом та нейтралізацією кіберінцидентів у державному секторі. Завдяки своїй технічній експертизі та правовому статусу ця служба є одним із базових операторів державної кібербезпеки [11].

Особливу функціональну роль у системі кібербезпеки виконує Служба безпеки України. Вона несе відповідальність за контррозвідувальний захист інформаційного простору, боротьбу з кібертероризмом, запобігання посяганням на критичну інфраструктуру держави, а також розслідування кіберзлочинів, що стосуються національної безпеки. До завдань СБУ належить виявлення й припинення діяльності іноземних спецслужб, які ведуть розвідувальну або деструктивну діяльність у кіберпросторі, протидія кібератакам на об'єкти з обмеженим доступом, захист каналів спеціального зв'язку, участь у розробці стратегії кібербезпеки та координація між суб'єктами безпекового сектору. В умовах гібридної війни та постійних кібератак з боку ворожих держав СБУ виконує критично важливу оперативно-аналітичну функцію, що дозволяє оперативно реагувати на загрози та нейтралізовувати їх на ранніх етапах [19].

Рада національної безпеки і оборони України є координаційним центром з питань безпеки, в тому числі й кібербезпеки. Як дорадчий орган при Президентові України, РНБО здійснює розробку стратегічних документів,

формує напрямки державної політики у сфері кіберзахисту та координує діяльність інших органів державної влади, які відповідають за інформаційну безпеку. Саме РНБО затверджує та оновлює Стратегію кібербезпеки України, проводить засідання щодо реагування на масштабні кіберінциденти, здійснює контроль за реалізацією національної політики у сфері цифрової безпеки. Завдяки широким повноваженням у сфері національної безпеки цей орган забезпечує міжвідомчу узгодженість дій та формує загальнодержавну позицію щодо протидії кіберзагрозам [17].

Суттєву роль у реалізації державної політики в інформаційно-цифровій сфері відіграє Міністерство цифрової трансформації України. Цей орган, хоч і не є безпосереднім суб'єктом системи кібероборони, забезпечує реалізацію стратегії цифрової трансформації, упроваджує цифрові сервіси, розвиває інфраструктуру електронного урядування та відповідає за створення безпечного цифрового середовища для громадян. В межах своєї діяльності Мінцифри координує заходи з підвищення цифрової грамотності, організовує кампанії з інформування населення щодо кібергігієни, реалізує спільні проєкти з міжнародними партнерами в сфері кіберстійкості державного сектору. Також Мінцифри виступає розробником технічних стандартів і правил для IT-інфраструктури органів виконавчої влади, що мають прямий вплив на рівень загальної кібербезпеки [18].

Національна поліція України через підрозділи кіберполіції здійснює виявлення, фіксацію, розслідування та припинення правопорушень, що вчиняються з використанням інформаційних технологій. Основні напрями її роботи включають протидію шахрайству в мережі, виявлення незаконного втручання в комп'ютерні системи, боротьбу з поширенням шкідливого програмного забезпечення, знищенням або зміною даних, а також протидію порушенням у сфері обігу персональних даних. Кіберполіція веде оперативно-розшукову діяльність, співпрацює з іноземними правоохоронними структурами, здійснює експертизи цифрових носіїв, а також залучається до міжнародних операцій у сфері кіберзлочинності [3]. Важливою є її

просвітницька функція – підрозділи поліції проводять роз'яснювальні кампанії, беруть участь у навчальних заходах та надають методичну допомогу у сфері кібербезпеки.

Міністерство оборони України та Генеральний штаб Збройних Сил України забезпечують кіберзахист у сфері національної оборони. У межах своїх функцій ці структури відповідають за створення військових спроможностей у сфері кібероборони, розробку і реалізацію оперативних сценаріїв протидії кіберзагрозам у період збройних конфліктів, а також захист мереж і систем, що використовуються у військовій сфері. Збройні Сили України активно формують власні кіберпідрозділи, готують спеціалістів у цій галузі та беруть участь у спільних навчаннях з партнерами, зокрема в межах співпраці з НАТО. Особливо важливою є діяльність кіберпідрозділів у період воєнного стану, коли кібератаки є частиною загальної стратегії агресії проти України [22].

Служба зовнішньої розвідки України реалізує завдання з добування, аналізу та надання керівництву держави розвідувальної інформації щодо потенційних кіберзагроз, які походять з-за кордону. Вона може брати участь у міждержавному обміні інформацією, моніторингу цифрової активності ворожих суб'єктів, а також формуванні аналітичних продуктів для стратегічного планування. Її діяльність, хоч і залишається непублічною, є важливою складовою національної системи протидії зовнішнім кібератакам [16].

Національний банк України, будучи регулятором банківської сфери, забезпечує кіберстійкість фінансової інфраструктури. Він визначає вимоги до кіберзахисту банківських систем, проводить аудит безпеки, організовує тренування щодо реагування на кіберінциденти, а також співпрацює з міжнародними фінансовими установами з метою уніфікації підходів до кібербезпеки в платіжному секторі. З огляду на високий рівень цифровізації фінансових послуг, саме банківський сектор є об'єктом підвищеного інтересу з боку кіберзлочинців і ворожих держав, що робить роль НБУ особливо значущою [9].

Таким чином, інституційна структура забезпечення кібербезпеки в Україні характеризується високим ступенем функціонального розмежування, але потребує постійного вдосконалення координації між суб'єктами. Діяльність Держспецзв'язку, СБУ, РНБО, Нацполіції, ЗСУ, Мінцифри та інших органів формує багаторівневу модель управління цифровою безпекою. Успішність реалізації державної політики у цій сфері залежить від ефективної взаємодії між суб'єктами, швидкості реагування на нові загрози, а також адаптації управлінських рішень до динамічного середовища кіберпростору.

2.3. Вплив війни на трансформацію політики кібербезпеки (з 2022 року)

Збройна агресія Російської Федерації проти України, що розпочалася у 2014 році та набула повномасштабного характеру з лютого 2022 року, суттєво змінила уявлення про природу сучасної війни, в якій традиційні воєнні дії поєднуються з інформаційними, психологічними, економічними та кібернетичними атаками. У зв'язку з цим, кіберпростір перетворився на одне з основних полів бойових дій, а забезпечення кібербезпеки стало не лише технічним чи інфраструктурним завданням, але й елементом стратегії національної безпеки в умовах воєнного часу.

Кіберпростір виявився ключовим середовищем для ведення гібридної війни, зокрема через активне використання кібератак для виведення з ладу інфраструктури, деморалізації населення, знищення або підміни критично важливої інформації, а також для здійснення впливу на внутрішню політичну стабільність країни. Відтак, державна політика у сфері кібербезпеки зазнала глибокої трансформації, що проявилась у переосмисленні пріоритетів, зміні організаційних моделей управління, посиленні нормативного регулювання та переорієнтації з переважно превентивного на переважно оборонний та реактивний характер.

Насамперед, трансформація політики кібербезпеки в умовах війни виявилася у зміні стратегічного бачення цифрової безпеки. Якщо до початку повномасштабного вторгнення основний акцент робився на розвитку цифрової інфраструктури, підвищенні кіберстійкості державних органів та впровадженні цифрових сервісів, то з 2022 року центр ваги перемістився на забезпечення обороноздатності в кіберпросторі, включаючи створення умов для стійкої роботи критичної інфраструктури, запобігання техногенним катастрофам внаслідок кібератак, а також протидію зовнішньому інформаційному втручанню.

В умовах агресії держава була змушена впровадити нові управлінські моделі реагування на кіберзагрози, що базуються на принципах швидкого реагування, автономності та адаптивності. Були активізовані дії урядових команд реагування на комп'ютерні інциденти, запроваджено цілодобове чергування в режимі надзвичайної ситуації, модернізовано системи моніторингу мереж. Стали звичними сценарії зміни маршрутів комунікації в реальному часі, миттєвого перемикання серверів, ізоляції заражених сегментів мережі, запуску резервних центрів обробки даних. Крім того, особливу роль відіграла добровольча кіберспільнота – зокрема, об'єднання на кшталт ІТ-армії України, яка почала координовано атакувати інформаційні ресурси країни-агресора, вести спостереження за пропагандистськими мережами та передавати технічну інформацію про потенційні уразливості ворожих систем [39].

Війна зумовила й прискорене впровадження концепції децентралізації кіберінфраструктури. Окремі елементи державного цифрового середовища були переведені в хмарні середовища, в тому числі на іноземні сервери з високим рівнем безпеки. Таке рішення дало змогу убезпечити критично важливі дані від фізичного знищення у разі атак на дата-центри або адміністративні будівлі. Водночас постала потреба у створенні гнучкої, резервної архітектури для державного управління в умовах надзвичайних ситуацій, що зумовило запровадження інструментів цифрової мобільності, включно з використанням зашифрованих VPN-з'єднань, резервних центрів

ухвалення рішень та платформ дистанційного управління державними процесами [41].

У контексті війни особливого значення набуло міжнародне співробітництво у сфері кібербезпеки. Україна отримала безпрецедентну підтримку з боку міжнародних партнерів, включаючи держави-члени ЄС і НАТО, транснаціональні технологічні компанії та неурядові організації. Компанії, такі як Microsoft, Google, Amazon, надавали хмарні ресурси, експертні консультації та послуги із захисту державних систем [31]. За підтримки урядів іноземних країн були проведені спільні навчання, виявлені та нейтралізовані масштабні кібершкідливі кампанії, що координувалися з території Росії та її союзників. Такі обставини сприяли посиленню позиції України як повноцінного учасника глобальної кіберкоаліції країн демократичного світу.

Війна також стимулювала поглиблення міжвідомчої координації у сфері кібербезпеки. Національна система реагування на кіберінциденти стала більш інтегрованою: Служба безпеки України, Державна служба спеціального зв'язку та захисту інформації, Міністерство оборони, Національна поліція та інші суб'єкти обмінюються оперативною інформацією у реальному часі, діють згідно з уніфікованими протоколами реагування та узгоджують свої дії з РНБО, яка виконує роль стратегічного координатора. Значну роль відіграє також Міністерство цифрової трансформації, яке забезпечує реалізацію цифрової стійкості на цивільному рівні, координує захист електронних сервісів, систем електронного урядування та цифрових платформ.

На тлі воєнних дій було активізовано й процеси оновлення нормативно-правової бази у сфері кібербезпеки. Зокрема, ініційовано зміни до Закону України «Про основні засади забезпечення кібербезпеки України», в частині уточнення функцій органів безпеки, уточнення категорій об'єктів критичної інфраструктури та посилення вимог до захисту державних інформаційних систем [10]. Було оновлено стратегію кібербезпеки з урахуванням реального бойового досвіду, акцент зроблено на формування проактивних

спроможностей, розвиток національної кіберрозвідки, впровадження моделі колективного кіберзахисту та створення систем раннього попередження. Запроваджено кримінальну відповідальність за нові види кіберактивності, у тому числі сприяння агресору через цифрові канали, кібершантаж, цифрове шпигунство, діяльність підконтрольних ворожих ІТ-груп.

Важливим викликом у період війни стало забезпечення кадрового потенціалу у сфері кібербезпеки. З одного боку, частина спеціалістів була мобілізована до лав Збройних Сил або виїхала з країни. З іншого боку, зросла потреба у фахівцях, здатних захищати критичну інфраструктуру, проводити експертизи, будувати архітектури захисту, координувати кризові ситуації. Це зумовило активізацію державних і приватних освітніх ініціатив, розширення програм підготовки в ІТ-сфері, створення спеціалізованих курсів з кібероборони та кризового управління, а також залучення до служби у кібервійськах волонтерів із відповідною кваліфікацією.

Таким чином, війна радикально змінила не лише операційні підходи до забезпечення кібербезпеки, але й саму філософію державної політики у цій сфері. Змістовним ядром трансформації стало усвідомлення, що кібербезпека є невід’ємною частиною загальної оборонної стратегії держави. Її забезпечення передбачає не лише технічний захист, а й політичну волю, стратегічне планування, законодавчу модернізацію, міжнародну співпрацю, кадрову підготовку та готовність діяти в умовах нестабільності. В умовах триваючої війни політика кібербезпеки дедалі більше інтегрується в усі рівні державного управління, стає пріоритетом національної стійкості та визначальним чинником виживання держави в цифрову епоху.

РОЗДІЛ 3.
ШЛЯХИ УДОСКОНАЛЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

3.1. Напрями модернізації нормативного регулювання кіберсфери

Постійне зростання кіберзагроз та розвиток цифрових технологій вимагають безперервного вдосконалення державної політики та нормативно-правового забезпечення у сфері кібербезпеки. В Україні, особливо в умовах гібридної агресії, актуально модернізувати нормативне регулювання кіберсфери з урахуванням найкращих світових практик та стандартів. Насамперед це передбачає гармонізацію національного законодавства із європейськими вимогами та міжнародними угодами. Зокрема, інтеграція норм нещодавно ухваленої директиви ЄС NIS2, яка встановлює підвищені вимоги до кібербезпеки для критично важливих секторів, сприятиме створенню узгодженої системи захисту [28]. Впровадження положень NIS2 в українське законодавство означає чіткіше визначення відповідальних сторін за кібербезпеку, обов’язкове повідомлення про серйозні інциденти та підзвітність за недотримання вимог безпеки. Таким чином, нормативна база набуде більш прогресивного, проактивного характеру, що відповідатиме сучасним викликам кіберпростору.

Одним із ключових напрямів модернізації є перехід від застарілих підходів до гнучких, ризик-орієнтованих методів регулювання. Раніше діяла комплексна система захисту інформації (КСЗІ), яка передбачала жорсткі стандартизовані вимоги до захисту державних інформаційних систем [12]. Проте в сучасних умовах такий уніфікований підхід виявився недостатньо ефективним і надто бюрократичним.

Сучасна державна політика робить акцент на управлінні кібербезпекою, заснованому на оцінці ризиків протягом життєвого циклу інформаційних систем. Кожна система чи сервіс мають отримувати індивідуальний профіль

захисту, що враховує їхні особливості, рівень критичності та актуальні загрози. Органи влади запроваджують механізми моніторингу та аудиту кібербезпеки, орієнтовані не на формальне виконання нормативів, а на досягнення реальних показників стійкості та зрілості систем захисту. Періодичні незалежні перевірки у поєднанні з самооцінками дозволять своєчасно виявляти вразливості та реагувати на них, мінімізуючи бюрократичні перепони. Такий динамічний підхід до нормативного регулювання забезпечує більшу адаптивність державної політики: правила і стандарти можуть оперативніше оновлюватися під появу нових технологій і типів атак.

Важливим аспектом оновлення нормативної бази є чітке визначення ролей і відповідальності всіх суб'єктів кібербезпеки. Новації в законодавстві України передбачають створення національної системи реагування на кібератаки, що включає розмежування рівнів реагування та запровадження спеціалізованих підрозділів кіберзахисту в державних установах і на критичній інфраструктурі. Закріплення таких структур на рівні закону забезпечує швидке та скоординоване реагування на інциденти, усуваючи дублювання функцій і прогалини у відповідальності. Кожен орган державної влади тепер зобов'язаний мати відповідального за кібербезпеку – впровадження посад фахівців, які опікуються внутрішньою політикою кіберзахисту, контролюють дотримання стандартів та взаємодіють з національними органами під час кризових ситуацій. Такий крок відповідає кращим міжнародним практикам, де наявність CISO (Chief Information Security Officer) або аналогічної посади є обов'язковою умовою кіберстійкості організації. В українському публічному секторі інституціоналізація функції кібербезпеки на керівному рівні сприятиме професіоналізації цієї сфери та зменшенню фрагментації підходів до захисту [34].

Окрім структурних змін, модернізація нормативного регулювання охоплює розвиток механізмів співпраці та обміну інформацією. Державна політика має стимулювати партнерство між державним і приватним секторами у протидії кіберзагрозам. Новітнє законодавство вже передбачає створення

єдиної системи обміну даними про кіберінциденти, що дозволить оперативно сповіщати усі зацікавлені сторони про атаки та вразливості. Встановлення обов'язкових процедур повідомлення і взаємодії, а також захист конфіденційності цих даних на законодавчому рівні, підвищить загальний рівень готовності до атак.

Глобальні інформаційні мережі обміну кіберзагрозами (threat intelligence sharing) потребують відповідного нормативного забезпечення, щоб Україна могла повноцінно брати участь у міжнародних програмах кіберзахисту. Крім того, на міжнародному рівні держава приєднується до ініціатив співробітництва – від участі у Будапештській конвенції про кіберзлочинність до поглиблення взаємодії з кіберцентрами НАТО та обміну даними з ЄС. Актуальним напрямом є укладення двосторонніх і багатосторонніх угод, що спростять екстрадицію кіберзлочинців та дозволять швидше отримувати інформацію про нові атаки. Невід'ємною складовою нормативної модернізації є також узгодження кібербезпекової політики із суміжними сферами, такими як захист персональних даних і протидія кіберзлочинності [23].

Україна вже робить кроки у цьому напрямі, оновлюючи законодавство про персональні дані відповідно до європейського регламенту щодо захисту даних (GDPR) та посилюючи відповідальність за кіберзлочини у Кримінальному кодексі. Ці зміни доповнюють загальну картину кібербезпеки, адже конфіденційність інформації та невідворотність покарання для зловмисників є важливими елементами стримування кіберзагроз. Отже, модернізація регуляторної сфери охоплює широкий спектр заходів – від внутрішніх реформ законів і стандартів до активної участі у світовій спільноті кібербезпеки. Усе це закладає підґрунтя для стійкого цифрового розвитку України, за якого держава здатна гнучко і завчасно реагувати на нові виклики кіберпростору.

3.2. Інтеграція інструментів цифрового урядування для підвищення кіберстійкості

Активний розвиток цифрового урядування відкриває нові можливості для підвищення кіберстійкості держави. Україна за останні роки зробила значний прорив у впровадженні електронних послуг та створенні сучасної цифрової інфраструктури: від запуску платформи «Дія» як «держави в смартфоні» до розбудови мережі національних електронних реєстрів. Ці інструменти цифрового урядування вже довели свою ефективність під час кризових ситуацій, забезпечивши безперервність надання послуг громадянам навіть в умовах воєнних загроз. Надалі важливо інтегрувати питання кібербезпеки безпосередньо в кожну цифрову ініціативу, щоб нові сервіси створювалися за принципом «security by design» [30]. Це означає, що при розробці державних інформаційних систем відразу враховуються вимоги захисту даних, стійкості до кібератак та забезпечення приватності користувачів. Впровадження міжнародних стандартів захищеності (наприклад, ISO 27001) при створенні електронних сервісів дозволить мінімізувати вразливості та підвищити довіру громадян до цифрового урядування.

Інтеграція інструментів цифрового урядування також передбачає використання сучасних технологічних рішень, що здатні посилити стійкість до кіберінцидентів. Одним з таких напрямів є перехід державних ІТ-систем на хмарні інфраструктури з високим рівнем захисту. Міжнародний досвід демонструє, що розміщення критичних даних і сервісів у хмарному середовищі, за умови використання шифрування та географічно розподілених дата-центрів, підвищує живучість систем при фізичних загрозах (наприклад, руйнуванні дата-центрів під час воєнних дій) [40]. Україна вже почала цей процес, співпрацюючи з глобальними технологічними компаніями для резервування копій державних реєстрів у захищених хмарних сховищах. Подальша цифровізація публічного сектору має супроводжуватися створенням резервних систем і дублюванням ключових сервісів в режимі реального часу, що

забезпечить безперервність управління у разі кібератак чи техногенних аварій. Наприклад, концепція «digital continuity» (цифрової безперервності) може бути реалізована через автоматичне переключення на резервні платформи, якщо основні державні онлайн-служби виходять з ладу.

Ще одним критично важливим інструментом кіберстійкості є впровадження єдиних стандартів цифрової ідентифікації та автентифікації в публічному секторі. Системи електронної ідентифікації громадян і чиновників, такі як BankID, MobileID чи інтегровані рішення в «Дії», повинні забезпечувати високий рівень довіри та захисту транзакцій. Використання двофакторної автентифікації, електронного підпису та інших засобів підтвердження особи зменшує ризики несанкціонованого доступу до державних інформаційних ресурсів. Крім того, розбудова сучасної системи керування доступом (IAM – Identity and Access Management) у державних органах дозволить централізовано контролювати права користувачів і оперативно виявляти підозрілі дії в мережах. Інтеграція таких інструментів цифрового урядування підсилює кібербезпеку «зсередини», роблячи державні системи менш вразливими до людського фактору та кібершпіонажу [6].

Водночас, розвиток цифрового урядування повинен супроводжуватися підвищенням обізнаності користувачів щодо кібербезпеки. Масова цифрова грамотність населення і державних службовців – необхідна передумова безпечного використання електронних послуг. Державні освітні проекти, такі як платформа «Дія.Цифрова освіта», мають включати курси з кібергігієни та навичок захисту даних. Це дозволить мінімізувати ризики соціальної інженерії та недбалого поводження з інформацією, оскільки навіть найдосконаліші технологічні системи можуть бути скомпрометовані через людський фактор. Таким чином, інтеграція інструментів цифрового урядування повинна йти паралельно з формуванням культури кібербезпеки серед усіх учасників цифрової екосистеми [8].

Підвищення кіберстійкості неможливе без налагодження ефективного моніторингу й обміну інформацією про загрози в режимі реального часу. Тут

також допомагають цифрові платформи урядування: створення єдиного центру моніторингу кібербезпеки (наприклад, державного SOC – Security Operations Center) забезпечить цілодобовий нагляд за мережами органів влади, автоматичне виявлення аномалій та координацію реагування [33]. Сучасні інструменти на основі штучного інтелекту та машинного навчання можуть аналізувати великий масив даних про мережевий трафік і події, виявляючи кібератаки на ранніх стадіях. Інтеграція таких систем в структуру державного управління дозволить більш ефективно протидіяти розвинутим персистентним загрозам.

Варто переймати найкращий міжнародний досвід: наприклад, Естонія, будучи піонером електронного урядування, паралельно впровадила передові засоби кіберзахисту, включно з технологією блокчейн для контролю цілісності даних та створенням «data embassy» – резервного серверного центру за кордоном на випадок втрати національних потужностей. Україна може використовувати подібні ідеї, комбінуючи швидкість і прозорість цифрових послуг з потужними механізмами безпеки та резервування. У підсумку, інтеграція інструментів цифрового урядування з урахуванням кібербезпеки створює синергетичний ефект: держава стає не лише більш ефективною в обслуговуванні громадян, але й більш стійкою до зовнішніх і внутрішніх кібернетичних викликів.

3.3. Пропозиції щодо впровадження системи стратегічного управління ризками в публічному секторі

Одним із найважливіших кроків до підвищення кіберстійкості є запровадження системи стратегічного управління ризиками кібербезпеки в публічному секторі. Ідея полягає в тому, щоб перейти від реактивного реагування на інциденти до проактивного виявлення та мінімізації потенційних загроз ще до того, як вони реалізуються. В умовах швидко зростаючої

складності атак державні установи повинні постійно оцінювати свій кіберризик – тобто ймовірність та можливі наслідки тих чи інших кібератак. Стратегічне управління ризиками означає, що на рівні керівництва організації приймаються зважені рішення щодо того, які ризики є прийнятними, а які потребують негайного реагування та додаткових ресурсів. Формування такої культури управління починається з усвідомлення: кіберризики несуть не лише технічні, а й значні управлінські та репутаційні загрози, і їх ігнорування може поставити під удар виконання державою ключових функцій.

Для впровадження дієвої системи управління ризиками необхідно, щоб кожен орган влади розробив власну стратегію кібербезпеки, базовану на оцінці ризиків. Практично це виглядає як циклічний процес: виявлення критичних інформаційних активів та можливих загроз для них, аналіз вразливостей та сценаріїв атак, оцінка впливу на роботу органу або надання послуг громадянам, визначення ймовірності реалізації загрози. На основі цього проводиться розрахунок рівня ризику та формується план реагування: набір заходів для зниження ризику до прийнятного рівня. Такими заходами можуть бути впровадження додаткових засобів захисту, резервування систем, підвищення рівня підготовки персоналу або навіть тимчасове відключення певних функцій до усунення вразливостей. Важливо, щоб ця діяльність не була одноразовою кампанією: управління ризиками має інтегруватися в повсякденну роботу установи. Для цього доцільно призначити відповідальних осіб чи комітети з управління ризиками, які регулярно переглядатимуть ризик-профіль організації, відстежуватимуть зміни в середовищі загроз і коригуватимуть стратегії захисту.

На національному рівні стратегічне управління кіберризиками вимагає координації та єдиних підходів. Доцільно розробити державні методичні рекомендації чи стандарти з оцінки кіберризиків для публічного сектору, щоб усі установи користувалися узгодженою методологією. Наприклад, можна адаптувати в українських реаліях міжнародно визнані підходи на кшталт NIST Cybersecurity Framework або стандартів ISO серії 27000, які приділяють значну

увагу управлінню ризиками. Єдиний підхід дозволить агрегувати дані про ризики з різних органів та формувати загальну картину кіберстійкості країни. Спеціалізований центральний орган (наприклад, Національний координаційний центр кібербезпеки) міг би збирати ці дані, визначати пріоритетні загрози на державному рівні та пропонувати уряду рішення щодо розподілу ресурсів для нейтралізації найбільш критичних ризиків. Впровадження такої вертикалі – від окремої установи до центру – забезпечить, що інформація про нові тактики атак чи вразливості швидко доводиться до всіх зацікавлених сторін, а реагування стає більш скоординованим.

Окрім процесів та структур, система стратегічного управління ризиками передбачає інвестування в людський капітал та зміну управлінського мислення. Керівники державних органів мають пройти відповідну підготовку з основ кіберризик-менеджменту, щоб розуміти мову ймовірностей та сценаріїв, на основі яких приймаються рішення. В Україні вже започатковані освітні програми для управлінців, що охоплюють тематику кібербезпеки і ризиків, зокрема курси для CDTO та IT-директорів у центральних органах влади [7]. Такі ініціативи слід розширювати, аби середній і вищий менеджмент публічного сектору формував навички проактивного оцінювання загроз. Одночасно варто стимулювати культуру відкритого обговорення ризиків: замість того, щоб приховувати вразливості через страх покарання, організації повинні мати стимули повідомляти про проблеми та спільно шукати рішення. Механізмами заохочення можуть стати як внутрішні програми відзначення підрозділів, що вчасно ідентифікували та зменшили ризики, так і державне рейтингування кіберстійкості органів влади.

Нарешті, стратегічний підхід до ризиків означає планування наперед різних варіантів розвитку подій. Публічний сектор має запровадити практику регулярних навчань та кібервправ для відпрацювання дій у разі масштабних атак. Сценарне планування («war-gaming») допоможе виявити слабкі місця в наявних протоколах та підготувати керівництво до прийняття рішень у стресових ситуаціях. Наприклад, моделювання атаки на енергетичну систему

чи систему е-урядування дозволить з’ясувати, чи готові відповідальні служби забезпечити резервні режими роботи, як комунікуватиметься з громадськістю та чи достатньо законодавчих повноважень для екстрених дій. Важливим елементом управління ризиками є також контроль ризиків постачальників та технологічних партнерів: державні установи повинні аналізувати надійність програмного і апаратного забезпечення, яке вони використовують, аби уникнути «троянського коня» у вигляді вразливостей у продукції недобросовісних виробників.

Результати усіх цих заходів мають повертатися в цикл управління ризиками – виявлені потенційні проблеми додаються до реєстрів ризиків, а плани дій оновлюються. Таким чином, утворюється замкнений цикл безперервного вдосконалення: загрози оцінюються, заходи реалізуються, ефективність перевіряється, і на основі зворотного зв’язку стратегія коригується.

Запровадження системи стратегічного управління ризиками перетворить кібербезпеку на невід’ємну частину державного управління, що дозволить державі випереджати можливі атаки і мінімізувати їхній вплив на суспільство.

ВИСНОВКИ

Проведене дослідження дало змогу сформулювати цілісне уявлення про сучасний стан, особливості та перспективи реалізації державної політики у сфері кібербезпеки в умовах цифрової трансформації та гібридної агресії. Встановлено, що кібербезпека стала критично важливою складовою системи національної безпеки, а ефективне функціонування органів публічної влади дедалі більше залежить від здатності протистояти кіберзагрозам та забезпечувати безпеку цифрової інфраструктури.

У межах кваліфікаційної роботи було проаналізовано нормативно-правову базу, інституційний механізм та стратегічні документи, що регулюють сферу кібербезпеки в Україні. Виявлено, що державна політика в цій галузі за останні роки зазнала суттєвих змін: модернізовано законодавчу основу, активізовано роботу ключових державних органів, розширено міжнародне співробітництво, а також інтегровано європейські стандарти. Зокрема, адаптація норм директиви NIS2 до українських реалій свідчить про прагнення гармонізувати підходи до кіберзахисту з вимогами Європейського Союзу.

Здійснено характеристику ролі основних суб'єктів кібербезпеки, зокрема Держспецзв'язку, СБУ, РНБО, Мінцифри, кіберполіції, Міноборони, Служби зовнішньої розвідки України та НБУ. Дослідження показало, що ефективна взаємодія між цими структурами має вирішальне значення для забезпечення цілісної та стійкої системи кіберзахисту. Разом з тим, наявні виклики свідчать про потребу подальшої координації міжвідомчих дій, створення єдиного центру моніторингу кіберінцидентів та впровадження ризик-орієнтованого підходу до управління.

У результаті аналізу виявлено низку проблем, які потребують системного розв'язання. Зокрема, зберігається фрагментарність нормативного регулювання, недостатній рівень кадрового забезпечення в сфері кіберзахисту, низький рівень обізнаності населення та державних службовців з питань кібергігієни, обмежені можливості оперативного реагування на складні атаки.

Ці проблеми набули особливої гостроти в умовах війни, коли кібератаки стали елементом воєнної стратегії ворога.

Результати дослідження можуть бути використані для удосконалення державної політики у сфері кібербезпеки, зокрема через:

– інтеграцію принципу «security by design» у всі цифрові ініціативи держави;

– розвиток хмарної інфраструктури з високим рівнем захисту;

– розбудову систем централізованого моніторингу та реагування (SOC);

– підвищення цифрової грамотності громадян і держслужбовців;

– створення нормативної бази для активної участі у міжнародних мережах обміну даними про кіберзагрози.

Отже, сформульовані у кваліфікаційній роботі положення мають практичну цінність для подальшої розбудови кіберстійкої держави та здатні лягти в основу реформування національної системи кібербезпеки в контексті євроінтеграції та збройного протистояння.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Директива (ЄС) 2016/1148 Європейського Парламенту і Ради від 6 липня 2016 р. про заходи для досягнення високого спільного рівня безпеки мережевих та інформаційних систем у межах Союзу. – Офіційний журнал ЄС. L 194, 19.7.2016, с. 2–3.

2. ДСТУ ISO/IEC 27032:2016 Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки (ISO/IEC 27032:2012, IDT). БУДСТАНДАРТ Online - нормативні документи будівельної галузі України. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 16.06.2025).

3. Кіберполіція України. Про департамент (офіційний сайт) / Національна поліція України. URL: https://cyberpolice.gov.ua/.

4. Конституція України: Законвід 28.06.1996 No254к/96-ВР. ВідомостіВерховноїРадиУкраїни (ВВР), 1996, No 30, ст. 141. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.

5. Кубанов Є. Теоретичні підходи до понятійно-категоріального апарату кібербезпеки в системі публічного управління / Є. В. Кубанов. – Черкаси : Міжрегіон. акад. управління персоналом, 2018. – Аспекти публічного управління. Т. 6, № 8. – С. 49–55.

6. Мойсак М. Які рішення кібербезпеки мають найбільший попит? // Комп’ютерне Обозрение. – 2023. – № 19. С. 2–3.

7. Навчальна програма «Кіберзахист державного органу: розроблення плану реагування на кіберінциденти» // Національне агентство України з питань державної служби (НАДС). – Київ, 6 травня 2025. URL: https://nads.gov.ua/news/u-nads-startuvala-navchalna-prohrama-z-kiberzakhystu-dlia-cdto-derzhavnykh-orhaniv.

8. Основи кібергігієни / Освітня серія на платформі «Дія.Освіта» – Офіційний курс. URL: https://osvita.diia.gov.ua/courses/cyber-hygiene.

9. Правління Національного банку України. Постанова від 15.02.2025 № 24 «Про організацію здійснення контролю за дотриманням банків системою інформаційної безпеки, кіберзахисту та електронних довірчих послуг» // Офіційний сайт НБУ. – Режим доступу: https://bank.gov.ua/admin_uploads/law/25022025_24.pdf?v=12.

10. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури : Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text

11. Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України : Постанова Каб. Міністрів України від 03.09.2014 № 411 : станом на 13 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/411-2014-п#Text

12. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/80/94-вр#Text

13. Про інформацію : Закон України від 02.10.1992 № 2657-XII : станом на 14 черв. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII : станом на 20 квіт. 2025 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

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

16. Про Службу зовнішньої розвідки України : Закон України від 01.12.2005 № 3160-IV : станом на 23 квіт. 2021 р. URL: https://zakon.rada.gov.ua/laws/show/3160-15#Text

17. Про Стратегію кібербезпеки України : Рішення Ради нац. безпеки і оборони України від 27.01.2016 : станом на 18 берез. 2016 р. URL: https://zakon.rada.gov.ua/laws/show/n0003525-16#Text

18. «Тиждень цифрової грамотності» / MediaSapiens, 18.11.2024. URL: https://ms.detector.media/kiberbezpeka/post/36746/2024-11-18-tyzhden-tsyfrovoi-gramotnosti-vid-mintcyfry-pokrashchuiemo-navychky-z-kibergigiieny

19. Федорчук Н. Діяльність СБУ в контексті національної безпеки: особливості кібербезпеки // Науковий вісник УжНУ. – 2024. – № 37-1. – 5 С.

20. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace / Європейська Комісія і Високий Представник із закордонних справ та безпеки, 2013.

21. Atlantic Council. The US National Cybersecurity Strategy Mark-Up. 2 March 2023. URL: https://www.atlanticcouncil.org/content-series/tech-at-the-leading-edge/the-us-national-cybersecurity-strategy-mark-up/

22. Communications and Cybersecurity Troops of the Armed Forces of Ukraine / Ministry of Defence of Ukraine. URL: https://mod.gov.ua/en/about-us/communications-and-cyber-security-troops.

23. Council of Europe – Cybercrime Division. Parties/Observers to the Budapest Convention on Cybercrime. URL: https://www.coe.int/en/web/cybercrime/parties-observers.

24. CSIRTs Network – ENISA. The Computer Security Incident Response Teams Network. URL: https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network.

25. Cybersecurity and Infrastructure Security Agency. Information Sharing - Cyber Threats and Advisories. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing.

26. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) // Official Journal of the European Union. L 333, 27.12.2022, p. 80–82.

27. European External Action Service (EEAS). 3rd Cyber Dialogue with the European Union takes place in Brussels. URL:

https://www.eeas.europa.eu/eeas/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels_en.

28. "EU's NIS2 Directive: What It Is, Its Purpose, and Why Ukraine Is Implementing It" / Cybersecurity & Infrastructure Protection Agency (CIP), урядовий портал. – 2 місяці тому. URL: https://cip.gov.ua/en/news/direktiva-yes-nis2-sho-ce-take-dlya-yakikh-potreb-rozroblena-ta-dlya-chogo-ukrayina-yiyi-implementuye.

29. Executive Order 14028. Improving the Nation’s Cybersecurity. The White House, 12.05.2021. URL: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

30. First look: U.S. wants to help export Ukraine's e-governance app to other countries / Axios. – 18 січня 2023. – [News article]. – Режим доступу: https://www.axios.com/2023/01/18/ukraine-app-diia-other-countries-usaid.

31. How Ukraine's Cyber Resilience: Centralised and grassroots / Hromada. – 10 серпня 2024. URL: https://hromada.network/ukraines-cyber-resilience-centralised-and-grassroots/.

32. ISO/IEC 27032:2012 – Information technology – Security techniques – Guidelines for cybersecurity / ISO & IEC. – Geneva : International Organization for Standardization / International Electrotechnical Commission, 2012. URL: https://www.iso.org/obp/ui/#iso:std:iso-iec:27032:ed-1:v1:en.

33. Kitsoft запускає центр кіберзахисту для державних сайтів (GovTech) / DigitalState.ua, 25 квітня 2025. URL: https://digitalstate.gov.ua/…/kitsoft-zapuskaye-tsentr-kiberzakhystu-dlia-derzavnykh-saytiv.

34. Lexology (Asters). Ukraine Enacts New Cybersecurity Law / 22 травня 2025. URL: https://www.lexology.com/library/detail.aspx?g=5ba8d445-97be-4aa8-a53e-32dc64459b4c.

35. NATO Communications and Information Agency (NCIA). NATO Computer Incident Response Capability (NCIRC) reaches full operational capability. – URL: https://www.ncia.nato.int/about-us/service-portfolio/nato-cyber-security-centre.

36. NATO Recognises Cyberspace as a "Domain of Operations" at Warsaw Summit / North Atlantic Treaty Organization. – Warsaw : 8–9 July 2016.

37. NATO Summit Wales 2014 : Summit Declaration / Heads of State and Government of the North Atlantic Treaty Organization. – Newport, Wales : 4–5 September 2014. – Підтвердження: кіберзахист визнається частиною колективної безпеки (Article 5).

38. Ottis R. Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective / Rain Ottis. – Tallinn : NATO Cooperative Cyber Defence Centre of Excellence, 2008. – 10 p.

39. Russian's War in Ukraine: Examining the Success of Ukrainian Cyber Defences / International Institute for Strategic Studies (IISS). – March 2023. – URL: https://www.iiss.org/research.

40. The Internet Under Attack: Internet resilience in Ukraine / Chatham House, серпень 2024. URL: https://www.chathamhouse.org/2024/08/internet-under-attack.

41. Ukraine's Digital Transformation: Innovation for Resilience / Harvard Kennedy School CID. 2 квітня 2025. URL: https://www.hks.harvard.edu/centers/cid/voices/ukraines-digital-transformation-innovation-resilience.

42. U.S. Department of Justice. Justice Department Charges 12 Chinese Contract Hackers and Law Enforcement Officers (3 months ago). URL: https://www.justice.gov/opa/pr/justice-department-charges-12-chinese-contract-hackers-and-law-enforcement-officers-global.

43. U.S. Government Accountability Office (GAO). Federal Response to SolarWinds and Microsoft Exchange Incidents. GAO-22-104746, квітень 2022. URL: https://www.gao.gov/assets/gao-22-104746.pdf.