Адміністративне право і процес

УДК 351:004.056

DOI https://doi.org/10.5281/zenodo.20374365

Стратегічні напрями розвитку системи державного управління у сфері цифрової безпеки

Татарнікова Тетяна Олександрівна,
кандидат юридичних наук, заступник начальника Центру судових і спеціальних експертиз, Український науково-дослідний інститут спеціальної техніки та судових експертиз Служби безпеки України, м. Київ, Україна, https://orcid.org/0000-0002-5470-8288

Карпінська Наталія Володимирівна
доктор юридичних наук, професор кафедри кримінального правосуддя і правоохоронної діяльності, Волинський національний університет імені Лесі Українки, м. Луцьк, Україна, https://orcid.org/0000-0001-9658-3623

Палюх Андрій Ярославович
доктор юридичних наук, доцент кафедри історії України, археології та спеціальних галузей історичних наук, Тернопільський національний педагогічний університет ім. Володимира Гнатюка, м. Тернопіль, Україна, https://orcid.org/0000-0001-9856-9147

Прийнято: 08.05.2026 | Опубліковано: 25.05.2026

Анотація: У статті досліджуються стратегічні напрями розвитку системи державного управління у сфері цифрової безпеки в умовах стрімкої

трансформації та зростання кіберзагроз. Мета дослідження полягає в обґрунтуванні стратегічних напрямків вдосконалення системи державного управління у сфері цифрової безпеки з метою підвищення її ефективності, узгодженості та стійкості до сучасних кіберзагроз. Методи дослідження містять системний та структурно-функціональний аналіз, порівняльний метод, узагальнення наукових підходів, а також аналіз нормативно-правових актів та сучасних публікацій у сфері цифрової безпеки та державного управління.

Результати дослідження свідчать, що сучасна система державного управління у сфері цифрової безпеки характеризується фрагментарністю, недостатнім рівнем координації між інституціями та нерівномірністю впровадження цифрових технологій. Разом з тим, визначено ключові виклики, найперше пов’язані зі зростанням складних кіберзагроз, гібридних атак, швидкої еволюції цифрового середовища та недостатнім рівнем розвитку кадрового забезпечення.

Обґрунтовано необхідність переходу до проактивної моделі кіберстійкості, яка передбачає використання інноваційних технологій, зокрема штучного інтелекту, великих даних та сучасних систем прогнозування ризиків. Запропоновано стратегічну класифікацію напрямів розвитку системи державного управління у сфері цифрової безпеки за рівнями кіберстійкості: базовим, адаптивним та проактивним. Такий підхід дозволяє систематизувати управлінські пріоритети відповідно до рівня готовності держави до кіберзагроз. Його впровадження сприяє підвищенню ефективності реагування на інциденти та формуванню довгострокової стратегії цифрової безпеки.

У висновках підтверджено, що ефективний розвиток системи державного управління у сфері цифрової безпеки можливий за умови комплексної інтеграції інституційних, технологічних та правових механізмів. Перехід до адаптивної та проактивної моделі управління розглядається як головна передумова підвищення стійкості держави до сучасних кіберзагроз та забезпечення стабільного функціонування цифрового середовища.

ISSN: 3041-2110

Ключові слова: цифрова безпека, кібербезпека, стратегія, стратегічне управління, інституційний розвиток, штучний інтелект, великі дані.

Strategic directions of development of the public administration system in the field of digital security

Tetiana Tatarnikova,
PhD in Sciences of Law, Deputy Head of the Center of Forensic and Special Expertises, Ukrainian Scientific and Research Institute of Special Equipment and Forensic Expertise of the Security Service of Ukraine,
Kyiv, Ukraine, https://orcid.org/0000-0002-5470-8288

Nataliia Karpinska,
Doctor of Law, Professor of the Departament of Craminal Justice and Law Enforcement, Lesya Ukrainka Volyn National University
Lutsk, Ukraine, https://orcid.org/0000-0001-9658-3623

Andriy Palyukh,
Doctor of Science of Law, Docent of the Department of History of Ukraine, Archaeology and Special Branches of Historical Sciences,
Ternopil National Pedagogical University Volodumur Gnatjuk
Ternopil, Ukraine, https://orcid.org/0000-0001-9856-9147

Abstract: The article examines the strategic directions of the development of the public administration system in the field of digital security in the conditions of rapid transformation and growth of cyber threats. The purpose of the study is to substantiate the strategic directions of improving the public administration system in the field of digital security in order to increase its efficiency, coherence and resilience to modern cyber threats. The research methods include systemic and

structural-functional analysis, comparative method, generalization of scientific approaches, as well as analysis of regulatory acts and modern publications in the field of digital security and public administration.

The results of the study indicate that the modern public administration system in the field of digital security is characterized by fragmentation, insufficient level of coordination between institutions and uneven implementation of digital technologies. At the same time, key challenges are identified, primarily related to the growth of complex cyber threats, hybrid attacks, rapid evolution of the digital environment and the insufficient level of human resource development.

The need to transition to a proactive model of cyber resilience is substantiated, which involves the use of innovative technologies, in particular AI, big data and modern risk forecasting systems. A strategic classification of the directions of development of the state administration system in the field of digital security is proposed according to the levels of cyber resilience: basic, adaptive and proactive. This approach allows systematizing management priorities in accordance with the level of readiness of the state to cyber threats. Its implementation contributes to increasing the efficiency of responding to incidents and forming a long-term digital security strategy.

The conclusions confirm that the effective development of the state administration system in the field of digital security is possible provided that there is a comprehensive integration of institutional, technological and legal mechanisms. The transition to an adaptive and proactive management model is considered the main prerequisite for increasing the state's resilience to modern cyber threats and ensuring the stable functioning of the digital environment.

Keywords: digital security, cybersecurity, strategy, strategic management, institutional development, artificial intelligence, big data.

Постановка проблеми. Етап цифрової трансформації державного управління, який невпинно триває останнім часом, зумовлений стрімким

впровадженням інформаційно-комунікаційних технологій у всі сфери суспільного життя, зокрема й у сферу надання адміністративних послуг, функціонування державних реєстрів, системи електронного урядування та управління критичною інфраструктурою. Окрім того, зростання рівня цифровізації суспільства супроводжується підвищенням кіберризиків, створюючи нові виклики для забезпечення національної безпеки. У рамках цього значної уваги набуває проблема формування ефективної системи державного управління у сфері цифрової безпеки, здатної забезпечити належний рівень захисту інформаційних ресурсів. Наявні організаційно-управлінські механізми та нормативно-правова база не в повній мірі відповідають сучасним викликам, що зумовлює необхідність їх вдосконалення відповідно до міжнародних стандартів та досвіду.

Загалом, наукове осмислення обраного питання потребує насамперед визначення стратегічних напрямів розвитку державного управління у сфері цифрової безпеки, що має важливе значення як для підвищення ефективності функціонування державних інституцій, так і для збереження стійкості держави перед сучасними кіберзагрозами.

Аналіз останніх досліджень і публікацій. Питання розвитку державного управління у сфері цифрової безпеки активно досліджується в сучасній науковій літературі. У наукових працях С. Лисенко [2] зосереджено увагу на інституційних аспектах формування системи інформаційної безпеки держави та необхідності вдосконалення управлінських механізмів, зважаючи на сучасні загрози. Дослідження С.О. Вовкотруб [4] поглиблюють аналіз викликів, пов’язаних із кібербезпекою, тим самим підсилюючи динамічних характер кіберзагроз та потребу в адаптивних підходах державної політики.

Практичні аспекти цифрової трансформації державних послуг розглядаються на прикладі платформи «Дія». Вказана платформа демонструє впровадження цифрових сервісів у систему державного управління. Дослідження Л. Стороженко, К. Андросової та Н. Галич [7] зосереджуються

на обґрунтуванні ролі штучного інтелекту (далі – ШІ) та цифрових технологій в підвищенні ефективності державного управління.

М. Ткач, С. Ясенко, Р. Бойко та Д. Дриньов [8] розглядають роль автоматизації та інформатизації в підвищенні ефективності сектору безпеки й оборони. Дослідження О. Пархоменко-Куцевіл [9] та А. Алієвої [11] підкреслюють значення цифрових стратегій для забезпечення національної безпеки в умовах сучасних загроз. Дослідник Є.О. Живило [10], [11] пропонує структуризацію національної стратегії кібербезпеки за конкретними ключовими напрямами, тим самим підкреслюючи важливість формування комплексного підходу в управлінні кіберризиками.

Попри значну кількість наукових напрацювань, недостатньо дослідженими залишаються питання формування цілісної моделі державного управління цифровою безпекою, а також інтеграції визначальних підходів до кіберстійкості. Саме ці аспекти розглядаються у межах даної статті як такі, що потребують подальшого наукового обґрунтування.

Виділення не вирішених раніше частин загальної проблеми. Низка наукових досліджень у сфері цифрової та кібербезпеки, а також частина важливих аспектів державного управління залишаються недостатньо розробленими. Так, подальшого вивчення потребують питання формування цілісної моделі державного управління цифровою безпекою, забезпечення ефективної координаційної діяльності, інтеграція державного та приватного секторів у процеси кіберзахисту.

Недостатньо дослідженими залишаються також механізми стратегічного планування розвитку цифрової безпеки із врахуванням сучасних гібридних загроз та стрімкого розвитку інноваційних технологій. Головною причиною такого стану є стрімка динаміка цифрового середовища, яка ускладнює своєчасне оновлення наукових підходів, а також фрагментарний характер досліджень, які насамперед зосереджуються на технічних аспектах кібербезпеки, лишаючи поза увагою інституційні та управлінські процеси.

Разом з тим, недостатній рівень узагальнення міжнародного досвіду та його адаптації до національних умов обмежують можливості формування ефективної державної політики в обраному напрямі дослідження.

У науковій статті передбачається зосередити увагу на обґрунтуванні стратегічних напрямів розвитку системи державного управління у сфері цифрової безпеки. Окрім того звернемо увагу на вдосконалення інституційної структури, посиленні координації між суб'єктами, розвитком нормативно-правового забезпечення та впровадженням інноваційних підходів до управління кіберризиками.

Формулювання цілей статті (постановка завдання)

Мета дослідження полягає в комплексному обґрунтуванні стратегічних напрямів розвитку системи державного управління у сфері цифрової безпеки з метою підвищення її ефективності, узгодженості та стійкості до сучасних кіберзагроз.

Завданнями дослідження є:

- провести аналіз сучасного стану та проблеми функціонування системи державного управління у сфері цифрової безпеки;
- визначити ключові виклики та невирішені аспекти у забезпеченні цифрової безпеки на державному рівні;
- обґрунтувати напрями вдосконалення державного управління у сфері цифрової безпеки.

Виклад основного матеріалу дослідження. Цифровізація сучасного суспільства є одним із ключових чинників розвитку державного управління, яке зумовлює активне впровадження інформаційно-комунікаційних технологій у діяльність органів влади. Насамперед вона сприяє підвищенню ефективності управлінських процесів та якості надання адміністративних послуг на тлі постійного зростання кіберзагроз.

Розвиток державного управління свідчить про постійне існування напруженості між прагненням підвищити ефективність управлінських

процесів та необхідністю забезпечити підзвітність та участь громадян. Така взаємодія чинників є основою сучасного цифрового врядування [1].

На думку вченого С.О. Лисенко, виклики та загрози інформаційній безпеці держави зумовлені складною взаємодією технологічних, політичних та суспільних чинників. Кібератаки та гібридні форми агресії є значними викликами у сфері цифрової безпеки. Кібератаки, які часто здійснюються за підтримки державних структур, спрямовуються на критичні інформаційні системи. Це приводить до порушення функціонування базових послуг та зниження захищеності операцій у державному та приватному секторах. Гібридна агресія, маючи риси кібероперацій з традиційними та нетрадиційними методами впливу, передбачає дестабілізацію державних інституцій шляхом використання вразливих осередків в цифровому та інформаційному просторі.

Через значну геополітичну напруженість Україна є мішенню для кібершпигунства, атак з вимогами викупу чи поширення дезінформації через електронні інформаційні канали. Вказані дії спрямовані на порушення належного функціонування державних інформаційних систем, дестабілізацію суспільно-політичної ситуації та підрив довіри до державних інституцій [2, с. 355].

Цифрова безпека в системі державного управління охоплює стратегічні й практичні аспекти, спрямовані на захист даних та забезпечення цілісності функціонування цифрових сервісів. Зважаючи на зростання залежності державних послуг від інформаційно-комунікаційних технологій, гарантування безпеки таких систем має пріоритетний характер для підтримки суспільної довіри та належного захисту персональної інформації громадян.

Одним із ключових концептуальних підходів до забезпечення цифрової безпеки є принцип «безпеки за замовчуванням у проєктуванні», який передбачає інтеграцію механізмів захисту безпосередньо на етапі розроблення цифрових систем, а не як додаткового елемент після їх створення. Реалізація

 ISSN: 3041-2110

вказаного підходу передбачає проведення комплексної оцінки ризиків, застосування методів безпечного програмування та впровадження ефективних механізмів контролю доступу. Разом з цим, систематичне тестування безпеки протягом всього життєвого циклу інформаційних систем значно підвищує їхню стійкість перед потенційними кіберзагрозами чи неправомірним втручанням в діяльність певних інституцій [3, с. 209].

У сфері державного управління захист персональних даних розглядається як обов'язкова правова вимога та як ключовий чинник забезпечення суспільної довіри до цифрових сервісів держави. Дотримання регуляторних актів, в тому числі й Загального регламенту захисту даних (GDPR), визначає встановлення жорстких вимог до обробки персональної інформації. Реалізація окреслених вимог передбачає впровадження технічних та організаційних заходів захисту, серед яких чільне місце посідає шифрування даних, що забезпечує їх конфіденційність як під час передавання, так і при зберіганні. Поміж з тим, значна увага приділяється забезпеченню прозорості процесів обробки даних, що також сприяє підвищенню рівня контролю користувачів за власною інформацією та зміцненням довіри до державних цифрових платформ.

Безперечно, системи державного управління стають все більш залежними від цифрових технологій, а відтак, зазнають впливу кібератак. Недостатнє фінансування, нестача кваліфікованих кадрів та складність адаптації регуляторних вимог у цифровому просторі сприяють відкритості державних інформаційних систем перед кібератаками [4, с. 22].

Кіберзагрози постійно еволюціонують, при цьому атаки програм-вимагачів є однією із найсерйозніших загроз, які найчастіше використовують шахраї. Надто поширеними є фішинг та DDoS-атаки, які порушують роботу критичної інфраструктури. Це, своєю чергою, вказує на необхідність пошуку ефективних стратегій кібербезпеки в державному секторі управління. Захист персональних даних є одним із викликів в цифровому адмініструванні, що

потребує постійного моніторингу та оновлення механізмів безпеки з метою запобігання витокам чи шахрайському доступу [5, с. 122].

Група вчених, Л. Стороженко, К. Андросова та Н. Галич, наголошує, що впровадження інтелектуальних технологій у сфері публічного управління значно розширює його функціональні можливості, формуючи передумови для переходу від реактивної до проактивної моделі врядування. Штучний інтелект у державному секторі використовується за різними напрямами, зокрема й з метою автоматизації адміністративних процесів. Це охоплює застосування чат-ботів і віртуальних асистентів, які забезпечують постійну обробку звернень громадян, систем розпізнавання образів з метою пришвидшення перевірки документів, а також алгоритмів машинного навчання для оптимізації розподілу ресурсів. Наразі в Україні впроваджено ШІ-асистента в застосунку «Дія». Асистент надає консультаційну підтримку громадянам в отриманні державних послуг [6].

Аналітичні та прогнозні можливості систем штучного інтелекту дозволяють опрацьовувати великі обсяги даних з мето виявлення особливостей, прогнозування соціально-економічних процесів і раннього попередження небезпечних явищ. Вказані аспекти створюють передумови для переходу від реактивної моделі управління до превентивного підходу, зосередженого на запобіганні проблемам.

Персоналізація державних послуг на основі ШІ дозволяє налаштувати сервіси під потреби кожного громадянина із врахуванням його життєвих обставин. Разом з цим, інтелектуальні системи допомагають органам влади аналізувати складні ситуації, прогнозують наслідки і обирають найбільш ефективні варіанти дій після вчинення кібератаки. Технології великих даних допомагають аналізувати реальну поведінку громадян та бізнесу в режимі реального часу. Це робить державну політику більш обґрунтованою. Так, аналіз даних платформи «Дія» дозволяє виявляти проблеми із наданням

ISSN: 3041-2110

послуг, тим самим покращуючи їх якість, і налагоджуючи комунікацію з користувачем.

Блокчейн-технології підвищують прозорість та безпеку державних реєстрів. В Україні вони вже активно використовуються під час проведення електронних аукціонів «Прозоро» та при створенні цифрових реєстрів. Це сприяє зменшенню корупційних ризиків та підсиленню довіри громадян до державних сервісів.

Важливо підкреслити, що впровадження інтелектуальних технологій супроводжується низкою викликів, головна з яких – етичні проблеми, зокрема алгоритмічна упередженість і прозорість рішень, а також ризики, пов'язані із захистом особистих даних. Технологічні загрози пов'язують також із залежністю від ІТ-систем, помилками алгоритмів та недостатнім рівнем кібербезпеки. Організаційні складнощі проявляються в дефіциті цифрових компетентностей та опорі змінам. Правові ж проблеми стосуються недостатнього регулювання використання ШІ та невизначеності статусу автоматизованих рішень [7].

Держава повинна не лише реагувати на кіберінциденти, а й переосмислювати засади державного управління, інтегруючи до нього принципи кіберстійкості, цифрової суверенності, інформаційної гігієни та безпеки персональних даних [8, с. 229]. Вчена Пархоменко-Куцевіл вказує, що ключовою умовою ефективного реагування держави на сучасні виклики стала розробка та впровадження цілісної цифрової стратегії як системоутворюючого інструменту державної політики у сфері національної безпеки. Очікується, що вказана стратегія охоплюватиме не лише напрями цифрової трансформації, а й інтегруватиметься в основу державного функціонування – безпеки, економіки, освіти, охорони здоров'я, оборони, зовнішньої політики. Стратегія повинна розглядатися як комплексна управлінська рамка, яка поєднує інституційні, правові, технологічні, кадрові та міжнародні процеси [9, с. 120].

ISSN: 3041-2110

За сучасних умов визначено низку ключових викликів, які стримують розвиток цифровізації публічного управління у сфері національної безпеки України. Насамперед проблеми набули апогею після введення на території України воєнного стану. Серед основних бар'єрів необхідно виокремити фрагментарність цифрової інфраструктури, що проявляється у відсутності єдиного підходу до цифровізації державних органів, нерівномірному впровадженні IT-технологій, використанні застарілих чи незахищених систем. Низький рівень інтеграції інформаційних систем ускладнює ефективний обмін даними між установами, знижуючи вчасність і ефективність прийнятих управлінських рішень та підвищуючи ризик втрати чи дублювання інформації [10, с. 35].

Зважаючи на це, необхідно сформулювати низку стратегічних рекомендацій, спрямованих на створення стійкого, адаптивного та безпечного цифрового середовища у секторі нацбезпеки. Найперше, необхідно продовжувати розвиток спеціалізованих кіберструткур на базі ЗСУ, СБУ, Держспецзв'язку та інших відомств, спроможних здійснювати активну кібероборону, оцінку рівня загроз і вчасного прийняття рішень на національному та міжнародному рівнях. Разом з тим, важливим напрямом є посилення міжвідомчої взаємодії через створення інтегрованих цифрових платформ з метою обміну інформацією, спільного аналізу ризиків та узгодження управлінських рішень.

Необхідно й надалі продовжувати впроваджувати національні стандарти цифрової безпеки, які б ефективно впливали на технічні, організаційні та етичні аспекти використання цифрових технологій, а також передбачатимуть механізми сертифікації та аудиту. Важливу роль відіграє також створення єдиної платформи управління ризиками в умовах надзвичайних ситуацій, яка б інтегрувала інструменти прогнозування, реагування та координації на основі сучасних технологій, зокрема ШІ, хмарних сховищ чи геоінформаційних систем.

Окремої уваги потребує інвестування у розвиток людського капіталу через удосконалення системи цифрової освіти, підвищення кваліфікації державних службовців і розширення публічно-приватного партнерства у сфері кібербезпеки. Водночас цифрова трансформація має стати невід'ємною складовою процесів відновлення держави, забезпечуючи прозорість використання ресурсів, ефективність управління та контроль за реалізацією відбудовчих проєктів.

Отже, цифрова трансформація публічного управління у сфері національної безпеки виступає ключовим чинником забезпечення стійкості держави в умовах сучасних загроз. Відтак, впровадження інтегрованих цифрових рішень, удосконалення нормативно-правового забезпечення та розвиток кіберможливостей мають визначати стратегічні пріоритети державної політики як у період війни, так і в процесі післявоєнного відновлення [11, с. 172]. В умовах повномасштабної війни цифрова безпека перетворюється із окремого напряму державної політики у системоутворюючий елемент національної безпеки, що забезпечує безперервність функціонування держави, стійкість критичної інфраструктури, ефективність управлінських рішень в складних умовах [12, с. 295].

Сучасні етапи розвитку системи державного управління у сфері цифрової безпеки України функціонують в умовах перманентного кіберпротистояння, яке поєднує класичні кіберзагрози з елементами гібридної війни, тим самим зумовлюючи необхідність переходу від традиційної моделі кіберзахисту до проактивної моделі кіберстійкості – здатної адаптуватися та швидко відновитися після атак. Цифрові технології в державному управлінні теж зазнають трансформації, виконуючи не тільки сервісну функцію, але також є інструментами, на основі яких забезпечується низка важливих державних завдань, зокрема:

- забезпечується безперервність надання державних послуг;

ISSN: 3041-2110

- здійснюється координація дій органів влади та сектору безпеки й оборони;
- відбувається вчасне прийняття рішень на основі даних;
- вдосконалюється інформаційна протидія та стратегічні комунікації.

На основі опрацьованого важливо запропонувати концептуально новий підхід у формуванні стратегічних напрямів розвитку системи державного управління у сфері цифрової безпеки, що ґрунтується на рівнях кіберстійкості держави в умовах воєнного стану. Окреслений підхід передбачає розуміння системи державного управління як адаптивної багаторівневої моделі, де стратегічні напрями формуються відповідно до здатності системи протидіяти загрозам, пристосовуватися до їх змін чи діяти на випередження в процесі їх виникнення.

Наразі не вистачає моделі державного управління, яка б сприяла забезпеченню еволюційного розвитку системи державного управління від фрагментарного реагування до інтегрованого стратегічного управління кібербезпекою (таблиця1):

Таблиця 1

Класифікація стратегічних напрямів розвитку системи державного управління у сфері цифрової безпеки за рівнями кіберстійкості

Рівень	**Характеристика**	**Ключові стратегічні напрями**	**Управлінський фокус**
Базовий (реактивний)	Орієнтованість на протидію вже реалізованим загрозам	розвиток систем кіберзахисту; реагування на інциденти; захист критичної інфраструктури; нормативно-правове забезпечення	Стабілізація та мінімізація наслідків
Адаптивний	Пристосування до динаміки загроз та управління ризиками	інтеграція інформаційних систем; міжвідомча координація;	Підвищення стійкості системи

ISSN: 3041-2110

		управління кіберризиками; розвиток кадрових можливостей	
Проактивний	Випередження загроз і стратегічне прогнозування	використання ШІ та Big Data; кіберрозвідка; прогнозування загроз; розвиток публічно-приватного партнерства	Формування «безпеки на випередження»

Джерело: Укладено авторами

Запропонована класифікація стратегічних напрямів, структурована за рівнями кіберстійкості, формує новий підхід до розуміння розвитку системи державного управління у сфері цифрової безпеки. Її використання допомагає відійти від фрагментарного визначення пріоритетів та забезпечити їх узгодженість в межах єдиного логічного розвитку. Напрацьовані варіанти дали можливість не лише визначити ключові напрями цифровізації у сфері державного управління, а й їх місце в загальній системі трансформації державного управління.

Починаючи від 2022 року в Україні ухвалено кілька важливих законопроєктів, що стосуються активної протидії агресії у кіберпросторі, наданні хмарних послуг та розміщення у «хмарах» державних інформаційних ресурсів тощо. Плідна робота триває також і над розробкою низки нормативно правових актів, які встановлюють відповідальність ка кіберінциденти, посилюють захищеність від кібератак державних інформаційних ресурсів. Окрім того державна політика зосереджується над посиленням міжнародної співпраці. Наразі Україна визначила для себе декілька надійних партнерів, досвід яких можна використовувати у своїй діяльності. Це Агентство з кібербезпеки та безпеки інфраструктури США (CISA), Агентство ЄС з питань кібербезпеки (ENISA), Команда реагування на комп’ютерні надзвичайні події (CERT-EU) [13].

Оскільки кібербезпека є не лише технічним, а й суспільним викликом, держава займається розробленням та впровадженням Національної стратегії кібербезпеки, яка б забезпечувала системне узгодження цілей у сфері кібербезпеки із загальними пріоритетами цифрової трансформації держави. Такий підхід дозволяє не лише визначити ключові напрями державної політики, але й передбачити дієві механізми її реалізації, обґрунтувати потребу в необхідних ресурсах та забезпечити їх ефективне і раціональне використання.

Вчений Є.О. Живило узагальнену модель Національної стратегії кібербезпеки пропонує структурувати за сімома ключовими напрямами, кожен з яких визначає ключові аспекти формування стійкої та ефективної системи кібербезпеки держави [14, с. 23] (таблиця 2):

Таблиця 2

Пріоритетні напрями Національної стратегії кібербезпеки та їх зміст

№	Пріоритетні напрями	Зміст
1.	Управління	Формування ефективної системи координації кібербезпеки, чіткий розподіл повноважень та відповідальності, визначення уповноваженого органу, забезпечення підзвітності, ресурсного забезпечення та міжвідомчої взаємодії
2.	Управління кіберризиками	Впровадження ризик-орієнтованого підходу: оцінка загроз, формування реєстрів ризиків, розробка галузевих профілів, застосування єдиної методології та регулярне оновлення політики конфіденційності відповідно до змін середовища загроз
3.	Готовність та стійкість	Розвиток можливостей реагувати на кіберінциденти (CERT/CSIRT), створення планів реагування на небезпеку, налагодження обміну інформацією, проведення навчань та підвищення рівня кіберстійкості держав
4.	Критична інфраструктура та послуги	Ідентифікація та захист критичної інфраструктури, впровадження стандартів безпеки, забезпечення безперервності функціонування, розвиток державно-приватного партнерства й ризик-орієнтованого управління

ISSN: 3041-2110

5.	Розбудова спроможностей та обізнаність	Розвиток людського капіталу, освіта й професійна підготовка, підтримка досліджень та інновацій, підвищення кіберграмотності населення й формування культури кіберезпеки
6.	Законодавчі аспекти	Вдосконалення нормативно-правової бази, гармоонізація у відповідності до міжнародних стандартів, протидія кіберзлочинності, захист прав людини, розвиток механізмів розслідування кіберінцидентів
7.	Міжнародне співробітництво	Інтеграція у глобальну систему кібербезпеки, участь в міжнродних проєктах, обмін інформацією, розвиток кібердипломатії та спільне реагування на транснаціональні загрози

Джерело: Систематизовано авторами на основі джерела [15].

Отже, розвиток системи державного управління у сфері цифрової безпеки є складним та багатовекторним процесом, що потребує системного та міждисциплінарного підходу. Ефективність функціонування такого підходу залежатиме від рівня інтеграції інституційних, технологічних та нормативно-правових компонентів. У рамках цього, впровадження проактивної моделі кіберстійкості є ключовою передумовою забезпечення національної безпеки в умовах цифрової трансформації. Важливість розвитку міжвідомчої координації та публічного-приватного партнерства залежить від ефективності управлінських рішень, а застосування інноваційних технологій, зокрема ШІ, та великих обсягів даних сприятимуть переходу до превентивного управління кіберзагрозами.

Нині особливо важливо продовжувати розвивати кадровий потенціал та підвищувати рівень цифрових навичок державних службовців, оскільки без цього ефективне управління у сфері цифрової безпеки просто неможливе. Констатовано, що українське законодавство і надалі потрібно узгоджувати з міжнародними стандартами, оскільки це прямо впливає на рівень захищеності цифрового середовища. Оскільки сучасні виклики швидко змінюються, тому

й підходи до управління кіберризиками не можуть залишатися сталими, їх потрібно постійно переглядати та вдосконалювати.

Висновки.

Проведене дослідження дозволило узагальнити та обґрунтувати стратегічні напрями розвитку системи державного управління у сфері цифрової безпеки із врахуванням сучасних викликів і потреб підвищення ефективності, узгодженості та стійкості до кіберзагроз. Аналіз сучасного стану функціонування систем державного управління у сфері цифрової безпеки виявив низку системних проблем, зокрема фрагментарність управлінських рішень, недостатній рівень міжвідомчої координації та нерівномірність впровадження цифрових технологій у діяльність державних органів. Ці аспекти значно ускладнюють формування цілісної та ефективної моделі управління.

У процесі дослідження визначено ключові виклики у сфері цифрової безпеки, до яких належать стрімке зростання кіерзагроз, поява складних гібридних атак, недостатній рівень готовності інституційної та кадрової складової до ефективного реагування на них. Окремо наголошено на динамічності цифрового середовища, яке вимагає постійного оновлення управлінських підходів. Разом з тим, обґрунтовано основні напрями вдосконалення системи державного управління у сфері цифрової безпеки, які передбачають посилення координації між суб’єктами кібербезпеки, розвиток цифрових компетентностей кадрів, вдосконалення нормативно-правового забезпечення і впровадження сучасних технологій управління ризиками.

Таким чином, результати дослідження підтверджують доцільність переходу на більш адаптивну та проактивну модель державного управління у сфері цифрової безпеки, що дозволить підвищити її ефективність та запечпечити належний рівень захисту в умовах сучасних кіберзагроз.

Подальші дослідження доцільно зосередити на розробленні адаптивних моделей державного управління у сфері цифрової безпеки з урахуванням

динаміки сучасних кіберзагроз. Важливим напрямом є також удосконалення механізмів міжвідомчої координації та інтеграції інноваційних технологій, зокрема штучного інтелекту, у систему кіберзахисту. Окрему увагу варто приділити також розвитку цифрових компетентностей державних службовців та вдосконаленню нормативно-правового забезпечення у цій сфері.

Список використаних джерел

1. World Policy Hub. *The Evolution of Public Administration: Key Phases and Stages* : вебсайт. 2023. URL: https://surl.lu/xaueed (дата звернення: 01.04.2026).

2. Лисенко С. О. Розвиток системи державного управління інформаційною безпекою на сучасному етапі. *Право та державне управління*. 2023. Вип. 1. С. 351–357. DOI: https://doi.org/10.32782/pdu.2023.1.53.

3. Рябчинська О. П. Протидія кіберзагрозам національній безпеці України: інституційно-превентивна спроможність. *Науковий вісник Ужгородського національного університету*. 2025. Вип. 92(4). С. 206–214. DOI: https://doi.org/10.24144/2307-3322.2025.92.4.28.

4. Вовкотруб С. О. Цифрова безпека в системі державного управління: еволюція, виклики та перспективи розвитку. *Вчені записки ТНУ імені В. І. Вернадського*. 2025. Вип. 2. С. 20–27. DOI: https://doi.org/10.32782/TNU-2663-6468/2025.2/04.

5. Тарасюк А. В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки ТНУ імені В. І. Вернадського. Серія: юридичні науки*. 2020. Т. 31 (70). Ч. 2, № 2. С. 119–124. DOI: https://doi.org/10.32838/2707-0581/2020.2-2/23. URL: https://www.juris.vernadskyjournals.in.ua/journals/2020/2_2020/part_2/25.pdf (дата звернення: 01.04.2026).

6. Дія. Цифрова держава : офіційний вебсайт. URL: https://diia.gov.ua/ (дата звернення: 01.04.2026).

7. Стороженко Л., Андросова К., Галич Н. Інтелектуальні технології та інформаційна безпека: стратегічні орієнтири розвитку цифрового публічного управління. *Публічно-управлінські та цифрові практики*. 2025. Вип. 4(7). URL: https://journals.dut.edu.ua/index.php/public/article/view/3378/3254 (дата звернення: 01.04.2026).

8. Ткач М., Ясенко С., Бойко Р., Дриньов Д. Роль і місце систем автоматизації та інформатизації в розвитку потенціалу сектору безпеки та оборони. *Social Development and Security*. 2021. Т. 11, № 2. С. 222–230.

9. Пархоменко-Куцевіл О. Сучасні виклики національній безпеці в умовах цифрових викликів: державно-управлінський аспект. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2025. № 12. С. 116–123. DOI: https://doi.org/10.31470/2786-6246-2025-12-116-123.

10. Кириченко Г. В. Трансформація публічного управління у сфері інформаційної безпеки: теоретико-правовий аспект. *Modern Scientific Journal*. 2026. № 11(1). С. 30–38. DOI: https://doi.org/10.36994/2786-9008-2026-11-4.

11. Алієва А. А. Цифровізація публічного управління у сфері національної безпеки: світові тенденції та рекомендації для України. *Таврійський науковий вісник*. 2025. Вип. 25. С. 170–178. URL: https://tnv-econom.ksauniv.ks.ua/index.php/journal/article/view/710/677 (дата звернення: 01.04.2026).

12. Птахіна О. М. Державне управління забезпеченням національної безпеки в умовах воєнного стану. *Інтеграція науки та практики управління в умовах соціокультурних трансформацій*. Полтава, 2025. С. 293–297.

13. Національна кібербезпека в умовах війни: основні досягнення, плани та перспективи : вебсайт. URL: https://cip.gov.ua/ua/news/nacionalna-kiberbezpeka-v-umovakh-viini-osnovni-dosyagnennya-plani-ta-perspektivi (дата звернення: 01.04.2026).

14. Живило Є., Черноног О. Міжнародні кібернавчання LOCKED SHIELDS – 2022: проблемні питання підготовки сил оборони. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2022. Т. 43(1). С. 19–24. DOI: https://doi.org/10.33099/2311-7249/2022-43-1-19-24.

15. Живило Є. О. Пріоритетні напрями національної стратегії кібербезпеки в контексті інтеграції до трирівневої моделі кібероборони. *Державне будівництво*. 2025. Вип. 1(37). DOI: https://doi.org/10.26565/1992-2337-2025-1-17.