УДК 35.08
DOI: https://doi.org/10.31470/2786-6246-2025-12-116-123

Пархоменко-Куцевіл Оксана, *доктор наук з державного управління, професор, завідувач кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі*

Parkhomenko-Kutsevil Oksana, *Doctor of Science in Public Administration, Professor, Head of the Department of Public Administration and Management at Hryhorii Skovoroda University in Pereiaslav*

ORCID ID: https://orcid.org/0000-0002-0758-346X

СУЧАСНІ ВИКЛИКИ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В УМОВАХ ЦИФРОВИХ ВИКЛИКІВ: ДЕРЖАВНО-УПРАВЛІНСЬКИЙ АСПЕКТ

MODERN CHALLENGES TO UKRAINE'S NATIONAL SECURITY IN THE FACE OF DIGITAL CHALLENGES: STATE AND ADMINISTRATIVE ASPECT

Анотація. У статті систематизовані сучасні виклики національній безпеці України в умовах цифрової трансформації, зокрема: кіберзагрози з боку держав-агресорів; інформаційно-психологічні операції; недостатня кібербезпека критичної інфраструктури; загроза цифровій суверенності; недостатня правова та інституційна база; низька цифрова грамотність і культура безпеки; виклики до національної ідентичності; проблеми цифрової нерівності та маргіналізації; корупційні ризики у сфері цифрових трансформацій; критична залежність від іноземних технологій; цифрові виклики для оборони та безпеки; недосконалість механізмів міжнародної цифрової взаємодії; проблема кадрового голоду в сфері кіберзахисту.

Обґрунтована розробка та реалізація цілісної цифрової стратегії, яка має стати системоутворюючим інструментом державної політики у сфері національної безпеки. Така стратегія повинна не лише окреслювати загальні напрями цифрової трансформації країни, а й глибоко інтегруватися в усі критичні сфери державного функціонування – безпеку, економіку, освіту, охорону здоров'я, оборону та зовнішню політику. У цьому контексті цифрова стратегія має розглядатися не як окремий документ або набір технологічних ініціатив, а як інтегрована рамка державного управління, що об'єднує інституційну, правову, технологічну, кадрову та міжнародну компоненти. Зазначено, що важливим аспектом сучасного державного управління в умовах цифрових трансформацій є розвиток цифрової дипломатії як інструменту зовнішньополітичної діяльності, що дозволяє Україні зміцнювати свої позиції на міжнародній арені, вибудовувати системну взаємодію з європейськими та трансатлантичними партнерами, а також формувати спільні підходи до врегулювання поведінки в кіберпросторі. Важливо, щоб держава не лише захищала від цифрових атак, а й формувала спроможне, гнучке та інноваційне цифрове середовище, яке слугуватиме платформою для довгострокового розвитку. Стратегічне управління в умовах цифрових викликів має стати двигуном модернізації всієї системи публічного управління, забезпечуючи її адаптивність до нових технологічних, геополітичних і суспільних реалій.

Ключові слова: державне управління, національна безпека, інформаційна безпека, кібербезпека, виклики національній безпеці, цифрова трансформація, реформування, реформа.

Abstract. The article systematizes modern challenges to Ukraine's national security in the face of digital transformation, in particular: cyber threats from aggressor states; information and psychological operations; insufficient cybersecurity of critical infrastructure; threat to digital sovereignty; insufficient legal and institutional framework; low digital literacy and security culture; challenges to national identity; problems of digital inequality and marginalization; corruption risks in the field of digital transformations; critical dependence on foreign technologies; digital challenges for defense and security; imperfection of

mechanisms for international digital interaction; problem of personnel shortage in the field of cyber defense.

The author substantiates the development and implementation of a holistic digital strategy, which should become a system-forming instrument of state policy in the field of national security. Such a strategy should not only outline the general directions of the country's digital transformation, but also be deeply integrated into all critical areas of state functioning – security, economy, education, healthcare, defense and foreign policy. In this context, the digital strategy should be considered not as a separate document or a set of technological initiatives, but as an integrated framework of public administration, combining institutional, legal, technological, personnel and international components. An important aspect of modern public administration in the context of digital transformations is the development of digital diplomacy as a tool of foreign policy activity, which allows Ukraine to strengthen its positions in the international arena, build systemic interaction with European and transatlantic partners, as well as form common approaches to regulating behavior in cyberspace. It is important that the state not only protects against digital attacks, but also forms a capable, flexible and innovative digital environment that will serve as a platform for long-term development. Strategic management in the face of digital challenges should become the engine of modernization of the entire public administration system, ensuring its adaptability to new technological, geopolitical and social realities.

Keywords: public administration, national security, information security, cybersecurity, challenges to national security, digital transformation, reformation, reform.

Постановка проблеми. Актуальність дослідження сучасних викликів національній безпеці України в умовах цифрової трансформації обумовлена масштабними змінами, які відбуваються у сфері державного управління, інформаційної безпеки та суспільно-політичного розвитку. Цифрові технології дедалі глибше інтегруються в ключові сфери функціонування держави – від оборони та економіки до охорони здоров'я й освіти, – що, з одного боку, відкриває нові можливості для підвищення ефективності управлінських процесів, а з іншого – створює нові загрози, передусім у сфері кібербезпеки, інформаційних впливів та технологічної залежності.

Загрози національній безпеці в цифровому вимірі сьогодні мають гібридний характер: це і кібератаки на державні інформаційні ресурси, і деструктивні кампанії в соціальних медіа, спрямовані на дестабілізацію суспільства, і спроби вплинути на управлінські рішення через підрив довіри до державних інституцій. У цьому контексті державне управління відіграє вирішальну роль як механізм вироблення, координації та реалізації політики цифрової безпеки. Йдеться не лише про технічні заходи, а й про інституційно-правову спроможність держави адаптуватися до нових викликів, формувати політику цифрової стійкості, розвивати кадровий потенціал у сфері кіберзахисту та забезпечувати ефективну міжвідомчу і міжсекторальну взаємодію.

З урахуванням російської агресії проти України, проблема національної безпеки набуває особливої гостроти. Війна ведеться не лише на фронті, а й у кіберпросторі, де держава змушена постійно протидіяти зовнішньому втручанню, інформаційно-психологічним операціям, спробам паралізувати критичну інфраструктуру. Водночас зростає значення цифрового суверенітету як ключового аспекту національної безпеки: йдеться про захист цифрових кордонів, незалежність від зовнішніх цифрових платформ, розвиток національних інформаційних систем та підтримку власного IT-сектора.

Дослідження цифрових викликів у контексті державного управління є необхідним для розуміння того, як адаптувати управлінську модель держави до умов нової реальності. Це включає формування стратегічних підходів до цифрової трансформації, створення механізмів раннього попередження загроз, а також розробку сучасної системи реагування на кіберінциденти та забезпечення інформаційної безпеки громадян. Лише цілісний, системний та випереджальний підхід у сфері державного управління здатен забезпечити ефективну протидію цифровим загрозам і гарантувати стабільність функціонування держави в умовах невизначеності та посилення глобальних ризиків.

Аналіз останніх досліджень і публікацій. Основні проблеми, виклики, небезпеки національної безпеки, системи забезпечення національної безпеки, механізми формування національної безпеки аналізують В. Білий, О. Бодрук, В. Горбулін, С. Домбровська, Є. Кобко, В. Мунтян, В. Нікіфоренко, Г. Ситник, В. Торічний, Т. Яровой та ін. Водночас, не існує системних досліджень обґрунтування сучасних викликів національній безпеці України в умовах цифрових викликів.

Метою дослідження є системний аналіз сучасних викликів національній безпеці України в умовах цифрових викликів, обґрунтування цілісної цифрової стратегії забезпечення національної безпеки України в умовах цифрових викликів.

Виклад основного матеріалу. Сучасні виклики національній безпеці України в умовах цифрових трансформацій потребують системного, глибоко вивіреного державного управління, здатного оперативно адаптуватися до нових форм загроз. У XXI ст. цифровізація стала не лише засобом підвищення ефективності управлінських процесів, а й джерелом нових уразливостей, які ставлять під загрозу стабільність, суверенітет і функціонування держави. На тлі російської військової агресії, що супроводжується безперервними кібератаками, кампаніями з дезінформації, інформаційно-психологічним тиском та зламами критичних інфраструктур, питання цифрової безпеки постало як один з головних викликів національній безпеці України.

Цифрові виклики мають комплексний і гібридний характер. Йдеться не лише про зловмисні втручання в ІТ-системи органів влади, банків, енергетичних та телекомунікаційних компаній, а й про більш складні механізми впливу: маніпуляцію громадською думкою через соціальні мережі, втручання у виборчі процеси, компрометацію посадових осіб та стратегічних державних рішень. Усе це підриває довіру до державних інституцій, послаблює легітимність влади та порушує механізми демократичного контролю.

Сучасні виклики національній безпеці України в умовах цифрової трансформації є комплексними, багатовимірними та динамічними. Вони охоплюють як зовнішні, так і внутрішні чинники та стосуються як суто технологічної сфери, так і інституційного, політичного, соціального, економічного й гуманітарного контекстів. До зазначених викликів слід віднести, зокрема [1; 2; 3; 4; 5]:

по-перше, кіберзагрози з боку держав-агресорів: постійні хакерські атаки на державні органи, об'єкти критичної інфраструктури, системи управління енергетикою, водопостачанням, зв'язком; використання технологій шкідливого програмного забезпечення для шпигунства, саботажу, порушення стабільності; спроби зруйнувати довіру до урядових цифрових сервісів (наприклад, до платформи «Дія»);

по-друге, інформаційно-психологічні операції: масовані кампанії з дезінформації та маніпуляції громадською думкою через соцмережі, месенджери, фейкові сайти; використання ботів, тролів та deepfake-технологій для підриву єдності суспільства та довіри до влади; підрив легітимності національних інституцій, виборчих процесів та мобілізаційної спроможності держави;

по-третє, недостатня кібербезпека критичної інфраструктури: багато ключових об'єктів (ТЕС, ГЕС, лікарні, транспорт, енергетичні мережі) не мають повноцінного кіберзахисту; обмеженість технічних, фінансових та кадрових ресурсів для реалізації стандартів NIS2 (ЄС) або аналогічних практик НАТО;

по-четверте, загроза цифровій суверенності: використання іноземних цифрових платформ, хмарних сервісів, програмного забезпечення без гарантій конфіденційності; можливість зовнішнього контролю над українськими даними, включаючи персональні, урядові та оборонні;

по-п'яте, недостатня правова та інституційна база: наявна нормативна база не повною мірою враховує специфіку гібридних цифрових загроз; відсутність чітких процедур взаємодії між силовими структурами, приватним сектором і громадянським суспільством у разі кіберінцидентів;

ISSN 2786-6246 (print) ● ISSN 2786-9091 (online)

по-шосте, низька цифрова грамотність і культура безпеки: слабка підготовленість населення, чиновників і бізнесу до цифрових загроз; часте порушення базових принципів цифрової безпеки (використання слабких паролів, фішинг, незахищені з'єднання);

по-сьоме, виклики до національної ідентичності: технології ШІ та медіа-маніпуляцій використовуються для формування альтернативної історії, фейкових наративів про державність, мову, культуру; створення альтернативних цифрових спільнот, орієнтованих на зовнішніх гравців (зокрема, з боку рф);

по-восьме, проблеми цифрової нерівності та маргіналізації: відсутність рівного доступу до цифрових послуг у сільських, прифронтових чи деокупованих територіях; втрата частиною громадян можливості реалізовувати свої права в цифровому середовищі;

по-дев'яте, корупційні ризики у сфері цифрових трансформацій: недоброчесні цифрові тендери, маніпуляції з державними контрактами на кібербезпеку; можливість використання цифрових систем для зловживань (в тому числі в оборонній сфері);

по-десяте, критична залежність від іноземних технологій: вузький простір для власних технологічних розробок через відсутність національних платформ, обмежені можливості R&D; ризики блокування доступу до важливих сервісів під час конфлікту або тиску;

по-одинадцяте, цифрові виклики для оборони та безпеки: асиметричне використання безпілотників, ШІ, розвідувальних систем у бойових діях; загроза «розумних» кіберзброї, яка може виводити з ладу військову логістику або засоби зв'язку;

по-дванадцяте, недосконаліть механізмів міжнародної цифрової взаємодії: відсутність уніфікованих стандартів безпеки в міжнародному кіберпросторі; невизначеність щодо правового режиму цифрової агресії та колективної відповіді на неї (наприклад, у межах НАТО);

по-тринадцяте, проблема кадрового голоду в сфері кіберзахисту: недостатня кількість фахівців із кібербезпеки в держсекторі; відтік спеціалістів у приватний сектор або за кордон.

У відповідь на ці загрози держава має не лише оперативно реагувати на кіберінциденти, але й переосмислити засади державного управління, інтегруючи до нього принципи кіберстійкості, цифрової суверенності, інформаційної гігієни та безпеки персональних даних [6]. Державне управління в цій парадигмі повинно бути здатне:

- забезпечити координацію дій між усіма гілками влади та секторами (державним, приватним, громадським) у сфері цифрової безпеки;
- гарантувати функціонування критичної цифрової інфраструктури навіть в умовах широкомасштабного кібернападу;
- створити адаптивні нормативно-правові механізми, що здатні регулювати цифрову сферу у динамічному середовищі, зокрема щодо обігу даних, відповідальності за кіберзлочини, цифрової ідентифікації громадян;
- розвивати людський капітал у сфері кібербезпеки, зокрема систему державної освіти та професійної підготовки кадрів для публічного сектору;
- запроваджувати системи моніторингу, попередження та аналізу цифрових загроз із використанням штучного інтелекту та великих даних (big data);
- реалізовувати інформаційну політику, спрямовану на підвищення рівня цифрової обізнаності населення та протидію маніпулятивним наративам.

Однією з ключових умов ефективного реагування держави на сучасні цифрові виклики є розробка та реалізація цілісної цифрової стратегії, яка має стати системоутворюючим інструментом державної політики у сфері національної безпеки. Така стратегія повинна не лише окреслювати загальні напрями цифрової трансформації країни, а й глибоко інтегруватися в усі критичні сфери державного функціонування – безпеку, економіку, освіту, охорону здоров'я, оборону та зовнішню політику. У цьому контексті цифрова стратегія має розглядатися не як окремий документ або набір технологічних ініціатив, а як інтегрована рамка державного управління, що об'єднує інституційну, правову, технологічну, кадрову та міжнародну компоненти.

1. Фокус на національні пріоритети. Цифрова стратегія має чітко відповідати національним інтересам України, забезпечуючи синхронізацію між різними секторами та міністерствами. Вона повинна враховувати специфіку національної безпеки в умовах гібридної війни, особливо щодо кіберзахисту об'єктів критичної інфраструктури (енергетика, транспорт, комунікації), протидії дезінформації, забезпечення інформаційної безпеки та цифрових прав громадян. У сфері економіки стратегія має передбачати стимулювання цифрових інновацій, розвиток електронної комерції, підтримку стартапів, а також впровадження штучного інтелекту та автоматизації в державному секторі. Для системи освіти пріоритетом є формування цифрових компетентностей з початкових рівнів навчання та підтримка наукових досліджень в галузі кібербезпеки. У галузі оборони – створення кібервійськ, інтеграція цифрових платформ у військове управління. У зовнішній політиці – формування союзів з міжнародними цифровими акторами.
2. Сценарний аналіз ризиків. Однією з методологічних основ стратегії має стати сценарне планування, що дозволяє проєктувати можливі вектори розвитку подій у цифровому середовищі: від стрімкого технологічного прогресу до масових кібератак чи руйнівних інформаційних кампаній. Аналіз має включати як «базовий», так і «песимістичний» та «оптимістичний» сценарії, з урахуванням можливих внутрішніх (недофінансування, слабка кадрова база) та зовнішніх (агресія, санкційний тиск, технологічна ізоляція) чинників [7; 8]. У рамках кожного сценарію мають бути напрацьовані чіткі алгоритми дій, що дозволяють державі оперативно реагувати, мінімізуючи ризики й втрати.
3. Безперервний моніторинг кіберзагроз і технологічних змін. Цифрова стратегія повинна мати динамічний характер, адаптуючись до швидкоплинної природи цифрового середовища. Це потребує створення постійно діючих аналітичних центрів (наприклад, на базі РНБО, СБУ, МВС, Мінцифри), які здійснюватимуть моніторинг кіберзагроз, аналіз векторів атак, технічну експертизу нових технологій і розробку рекомендацій для оперативного коригування державної політики. Особливу увагу слід приділити загрозам з боку високорозвинених цифрових держав та приватних корпорацій, здатних впливати на національні процеси через технологічну залежність (інфраструктура, сервіси, апаратне забезпечення, програмне забезпечення).
4. Інтеграція міжнародного досвіду та партнерства. Україна не може протистояти цифровим викликам ізольовано. Надзвичайно важливим компонентом цифрової стратегії має стати міжнародна співпраця, зокрема з Європейським Союзом, НАТО, США, країнами Балтії, Японією, Кореєю. Йдеться про:
   - участь у міжнародних ініціативах кібербезпеки (наприклад, Budapest Convention);
   - співпрацю в межах Єдиного цифрового ринку ЄС;
   - залучення технічної підтримки та іноземних експертів;
   - використання програм фінансування та грантів (EU4Digital, Horizon Europe, USAID, тощо);
   - обмін даними та розвідкою про загрози, спільні тренування з реагування на кібератаки.

   Міжнародні партнери також можуть допомогти Україні у побудові державних цифрових сервісів, безпечної інфраструктури, підготовці кадрів та впровадженні стандартів кібергігієни.
5. Оцінка ефективності та стратегічна гнучкість. Цифрова стратегія має передбачати регулярну оцінку її реалізації, з використанням як кількісних (KPI), так і якісних індикаторів. Наприклад, кількість відбитих кібератак, час реакції на інциденти, рівень цифрових навичок населення, покриття державними е-сервісами тощо. Ці дані повинні бути доступними для громадськості в рамках прозорого державного управління. Окрему увагу слід приділити гнучкості стратегії – вона не повинна бути статичною, а має змінюватися в міру трансформації цифрового простору та появи нових викликів.

На нашу думку, цілісна цифрова стратегія національної безпеки України – це не просто технічний документ, а архітектура національного виживання та розвитку у цифрову епоху. Вона

забезпечує не лише безпеку, а й конкурентоспроможність, інноваційність та стійкість держави, дозволяючи Україні впевнено формувати своє цифрове майбутнє у контексті глобальної нестабільності та технологічних змін.

Важливим аспектом сучасного державного управління в умовах цифрових трансформацій є розвиток цифрової дипломатії як інструменту зовнішньополітичної діяльності, що дозволяє Україні зміцнювати свої позиції на міжнародній арені, вибудовувати системну взаємодію з європейськими та трансатлантичними партнерами, а також формувати спільні підходи до врегулювання поведінки в кіберпросторі. У сучасному цифровому світі, де кібератаки стають частиною гібридної війни, а цифрові технології впливають на політичні, економічні та безпекові процеси, цифрова дипломатія набуває статусу стратегічного ресурсу. Україна, перебуваючи в умовах постійної загрози з боку держави-агресора, зацікавлена у формуванні широкої міжнародної коаліції на підтримку принципів відповідального використання інформаційних технологій, захисту кіберпростору та запобігання зловживанням цифровими інструментами для дестабілізації суспільства чи втручання у внутрішні справи держав.

Цифрова дипломатія передбачає активну участь України у міжнародних дискусіях щодо встановлення правил і норм поведінки держав у кіберсередовищі, у тому числі в рамках ООН, ОБСЄ, ЄС, Ради Європи, а також у форматах двостороннього та багатостороннього співробітництва. Йдеться про вироблення та просування ініціатив щодо прозорості, відповідальності, заборони кіберагресії, недопущення цифрової цензури та захисту цифрових прав людини. Україна має зацікавленість у тому, щоб світове співтовариство визнавало акти кіберагресії як порушення міжнародного права, а також, щоб були встановлені механізми реагування на подібні акти, включно із санкційними інструментами.

У цьому контексті надзвичайно актуальною є гармонізація національної цифрової політики з правовими, технічними та етичними стандартами Європейського Союзу та НАТО, враховуючи стратегічний курс України на повноправне членство в цих структурах. З боку ЄС це означає поступове наближення до норм єдиного цифрового ринку, дотримання положень Загального регламенту із захисту персональних даних (GDPR), реалізацію Директиви NIS2 щодо кіберстійкості критичної інфраструктури, а також імплементацію положень Стратегії ЄС з кібербезпеки. З боку НАТО ключовим є приведення національного законодавства у відповідність до Стратегії кібероборони Альянсу, участь у тренуваннях та місіях з кіберзахисту, обмін інформацією та інтеграція в спільні механізми реагування на інциденти.

Крім правових аспектів, гармонізація вимагає також інституційної синхронізації – створення національних органів з чітко визначеними повноваженнями у сфері цифрової безпеки, участі в спільних міжурядових платформах, а також забезпечення прозорості та довіри між партнерами. Цифрова дипломатія передбачає і активну взаємодію з глобальними IT-корпораціями, які контролюють основну частину цифрової інфраструктури (Google, Microsoft, Amazon, Meta та ін.), адже саме через ці платформи можуть здійснюватися інформаційні операції, витоки даних чи порушення прав користувачів. Українська дипломатія має активно просувати принципи відповідальності таких суб'єктів та захисту національних інтересів у цифровій сфері.

Отже, цифрова дипломатія є не лише допоміжною складовою зовнішньої політики, а й ключовим інструментом забезпечення цифрової суверенності, кіберстійкості, інституційної сумісності з партнерами та довгострокової безпеки України в умовах глобалізованого інформаційного простору. Її розвиток потребує не лише політичної волі, а й фахової експертизи, системної підтримки з боку урядових структур і активного залучення наукової та громадянської спільноти.

Висновки. Проведений аналіз дає підстави зазначити, що у контексті стрімкої цифрової трансформації та гібридної війни, яку веде росія проти України, питання національної безпеки набуло нових змістових і управлінських вимірів. В умовах високотехнологічних ризиків, державне управління має трансформуватися з реактивної моделі в проактивну, яка здатна передбачати, запобігати й ефективно протидіяти цифровим загрозам. Цифрова сфера стала одним із головних

полів боротьби за державний суверенітет, стабільність інституцій та захист прав громадян. Кіберзагрози, інформаційно-психологічні операції, атаки на критичну інфраструктуру, підрив цифрової довіри – це не поодинокі інциденти, а системні виклики, які потребують відповідної архітектури управлінських рішень.

Успішне державне реагування вимагає комплексної цифрової безпекової політики, заснованої на інтеграції міжсекторальної взаємодії, правового оновлення, інституційної спроможності та міжнародного партнерства. Ключовим інструментом має стати національна стратегія кіберстійкості, яка повинна включати: системний моніторинг цифрового середовища, підготовку державних службовців та фахівців у сфері ІТ-безпеки, розбудову інфраструктури безпечного обміну даними, гармонізацію з європейськими й євроатлантичними стандартами, а також забезпечення прозорості та підзвітності цифрових перетворень.

Важливо, щоб держава не лише захищала від цифрових атак, а й формувала спроможне, гнучке та інноваційне цифрове середовище, яке слугуватиме платформою для довгострокового розвитку. Стратегічне управління в умовах цифрових викликів має стати двигуном модернізації всієї системи публічного управління, забезпечуючи її адаптивність до нових технологічних, геополітичних і суспільних реалій.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Новікова Н., Бойко Л. Цифровізація та національна безпека: тенденції та виклики. *Національна безпека: право та економіка*. 2024. № 1 (1). С. 72–77. http://doi.org/10.51369/3083-5917-2024-1-8
2. Домбровський Л.В. Інформаційна безпека держави у системі національної безпеки України. *Вісник національного університету цивільного захисту України.* 2024. URL: http://repositsc.nuczu.edu.ua/bitstream/123456789/20339/1/12Dombrovskyi.pdf (дата звернення: 09.03.2025).
3. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. №2. С. 200–203.
4. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Сер.: Державне управління.* 2022. Вип.2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (дата звернення: 09.03.2025).
5. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз: монографія. Київ: Ліра-К, 2020. 352 с.
6. 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. Том 11. № 2. С. 222–230.
7. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1. С. 20–26.
8. Пугачов О.І. Проблеми забезпечення інформаційної безпеки України в сучасних умовах. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2024. №12. https://doi.org/10.54929/2786-5746-2024-12-02-15

REFERENCES

1. Novikova, N. & Boiko, L. (2024). Tsyfrovizatsiia ta natsionalna bezpeka: tendentsii ta vyklyky [Digitalization and national security: trends and challenges]. *Natsionalna bezpeka: pravo ta ekonomika – National security: law and economics*, *1 (1),* 72–77. http://doi.org/10.51369/3083-5917-2024-1-8 [in Ukrainian].
2. Dombrovskyi, L.V. (2024). Informatsiina bezpeka derzhavy u systemi natsionalnoi bezpeky Ukrainy [Information security of the state in the national security system of Ukraine]. *Visnyk natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy – Bulletin of the National University of Civil Protection of*

Ukraine. Retrieved from http://repositsc.nuczu.edu.ua/bitstream/123456789/20339/1/12Dombrovskyi.pdf [in Ukrainian].
3. Havryltsiv, M.T. (2020). Informatsiina bezpeka derzhavy v systemi natsionalnoi bezpeky Ukrainy [Information security of the state in the national security system of Ukraine]. *Yurydychnyi naukovyi zhurnal – Legal Scientific Journal, 2,* 200–203 [in Ukrainian].
4. Leonenko, N.A. & Postupna, O.V. (2022). Informatsiina bezpeka Ukrainy: mekhanizmy, suchasni vyklyky ta zahrozy v umovakh informatsiinoho hlobalizmu [Information security of Ukraine: mechanisms, modern challenges and threats in the conditions of information globalism]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy. Ser.: Derzhavne upravlinnia – Bulletin of the National University of Civil Defense of Ukraine. eries: State Administration*, *2 (17*). Retrieved from http://repositsc.nuczu.edu.ua/handle/123456789/16883 [in Ukrainian].
5. Shemchuk, V.V. (2020). *Zabezpechennia informatsiinoi bezpeky yak funktsiia suchasnykh derzhav: porivnialno-pravovyi analiz: monohrafiia [Ensuring information security as a function of modern states: comparative legal analysis: monograph].* Kyiv: Lira-K [in Ukrainian].
6. Tkach, M., Yasenko, S., Boiko, R. & Drynov, D. (2021). Rol i mistse system avtomatyzatsii ta informatyzatsii v rozvytku potentsialu sektoru bezpeky ta oborony [The role and place of automation and informatization systems in the development of the potential of the security and defense sector]. *Social Development and Security – Social Development and Security, 11 (2),* 222–230 [in Ukrainian].
7. Zalievska, I.I. & Udrenas, H.I. (2022). Informatsiina bezpeka v Ukraini v umovakh rosiiskoi viiskovoi ahresii [Information security in Ukraine under conditions of Russian military aggression]. *Pivdennoukrainskyi pravnychyi chasopys – South Ukrainian Law Journal, 1,* 20–26 [in Ukrainian].
8. Puhachov, O.I. (2024). Problemy zabezpechennia informatsiinoi bezpeky Ukrainy v suchasnykh umovakh [Problems of ensuring information security in Ukraine under modern conditions]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia – Problems of modern transformations. Series: law, public management and administration*, *12.* https://doi.org/10.54929/2786-5746-2024-12-02-15 [in Ukrainian].

Подано до редакції 10.03.25 р.
Прийнято до друку 10.04.25 р.