

УДК 35.351: 338.22:355.02

DOI <https://doi.org/10.51547/ppp.dp.ua/2025.2.11>

Таран Євгеній Іванович,

кандидат політичних наук, доцент,

доцент кафедри глобальної та національної безпеки

Навчально-наукового інституту публічного управління та державної служби

Київського національного університету імені Тараса Шевченка

ORCID ID: 0000-0002-1822-6978

ЕЛЕКТРОННЕ УРЯДУВАННЯ ЯК ІНСТРУМЕНТ ПОБУДОВИ ПУБЛІЧНО-СЕРВІСНОЇ ДЕРЖАВИ В УМОВАХ ТРАНСФОРМАЦІЇ ДЕРЖАВНОЇ ПОЛІТИКИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

E-GOVERNANCE AS A TOOL FOR BUILDING A PUBLIC SERVICE STATE IN THE CONTEXT OF THE TRANSFORMATION OF NATIONAL SECURITY POLICY

У статті досліджується роль електронного урядування як ключового інструменту розбудови публічно-сервісної держави в умовах зміни державної політики національної безпеки. Актуальність цього дослідження зумовлюється глибокими трансформаційними процесами, котрі наразі відбуваються в системі публічного управління та безпеки в Україні. Мета статті – проаналізувати потенціал електронного урядування як інструменту розбудови публічно-сервісної держави та з'ясувати його роль у трансформації державної політики національної безпеки в умовах цифрової модернізації та актуальних безпекових викликів. Для виконання дослідження було застосовано низку загальнонаукових методів, таких як аналіз та синтез, системний підхід, порівняльно-правовий, формально-юридичний метод, емпіричний метод. Розглянуто поняття, суть та засади електронного урядування. З'ясовано концепцію публічно-сервісної держави та взаємозв'язок електронного урядування з публічно-сервісною моделлю державного управління. Підкреслено увагу на цифровізацію як фактор модернізації системи національної безпеки. Досліджено взаємозв'язок між електронним урядуванням та національною безпекою за умов зовнішніх та внутрішніх викликів. Проаналізовано теперішній стан впровадження електронного урядування в Україні. Зазначено ключові фактори, що формують міцну систему взаємодії між владою та громадянами, зменшують рівень соціальної напруги, протидіють корупції та сприяють стабільності політичної системи (прозорість, відкритість та довіра). Окрему увагу приділено захисту критичної інформаційної інфраструктури в умовах цифрового управління. Визначено шляхи посилення кібербезпеки та інформаційної протидії в контексті цифрової країни. Надано поради щодо вдосконалення електронних сервісів у царині безпеки. Охарактеризовано модель публічно-сервісної держави в умовах нової архітектури безпеки. Запропоновано напрями інтеграції електронного урядування в державну політику безпеки України. У висновках відзначено, що електронне урядування стає значущим інструментом гарантування прозорості, підзвітності та результативності влади, що є основними рисами публічно-сервісної моделі держави. Дослідження цієї теми дозволяє сформулювати цілісне уявлення ролі електронного урядування у системі національної безпеки, виявити можливі загрози, оцінити переваги цифровізації, а також напрацювати пропозиції щодо покращення державної політики з огляду на сучасні реалії та потреби суспільства.

Ключові слова: трансформація, цифровізація, електронне урядування, національна безпека, публічно-сервісна держава, кіберзахист, інтеграція, критична інфраструктура, архітектура безпеки.

The significance of this research is decided by the substantial transformation processes currently happening in the public administration and security system in Ukraine. In these conditions, e-government is not simply a tool for streamlining governance processes, but also a central means of augmenting the degree of safety of the nation – in cyber defense, crisis management, protection of the information space, and ensuring citizens' rights. During military conflict and post-war rebuilding, when security concerns are critical, finding balanced solutions between transparency of e-governance and protection of state interests is exceedingly urgent. Thus, a comprehensive scientific examination of the connection between e-government, the public-service model of the state, and the evolution of national security policy is crucial and opportune for the development of a contemporary, sustainable, and democratic Ukraine. The essay evaluates the function of e-government as a vital instrument for constructing a public-service state within the scope of changing national security policy. The aim of this paper is to explore the potential of e-government as a tool for establishing a public-service state and to determine its role in the transformation of the state national security policy, considering digital modernization and existing security challenges. To perform the study, several general scientific methodologies were utilized, like analysis and synthesis, systematic approach, comparative legal, formal legal method, and empirical method. The concept, essence, and principles of e-government are explored. The concept of a public-service state and the correlation of e-government with the public-service model of public administration are clarified. Emphasis

is placed on digitalization as a element in modernizing the national security system. The relationship between e-governance and national security concerning external and internal challenges is explored. The current state of e-government implementation in Ukraine is examined. The central factors that form a strong system of interaction between the government and citizens, lessen social tension, fight corruption, and encourage the stability of the political system (transparency, openness, and trust) are pinpointed. Specific focus is given to protecting crucial information infrastructure inside digital governance. Methods for strengthening cybersecurity and information countermeasures inside a digital nation are presented. Suggestions for improving electronic services in the security domain are provided. The model of a public service state, within the new security architecture, is detailed. The author proposes pathways for integrating e-government into Ukraine's State security policy. The concluding notes emphasize that e-governance is developing into an important instrument for furthering transparency, accountability and effectiveness of governance, fundamental characteristics of the public service model of the state. Examining this subject lets us build a comprehensive perspective of e-governance's role in the national security system, pinpoint potential dangers, evaluate the advantages of digitalization, and formulate suggestions for enhancing public policy considering present realities and societal requirements.

Key words: transformation, digitalization, e-government, national security, public service state, cyber defense, integration, critical infrastructure, security architecture.

Постановка проблеми. Електронне урядування все частіше працює як основний фактор у створенні нової моделі – публічно-сервісної держави, а не просто як інструмент для вдосконалення надання послуг громадянам. Водночас Україна стикається зі значними загрозами безпеки, кібератаками та інформаційною війною, яка потребує оновлення національної безпеки. У цьому контексті важливо дослідити суть електронного урядування як невіддільної частини системи державної безпеки з її роллю у забезпеченні прозорості, стабільності державних установ та підвищенню довіри громадян у владі.

Вивчення ролі електронного урядування як інструменту створення публічно-сервісної держави після реформи політики національної безпеки, зокрема, кілька його елементів активно розглядаються у роботах вітчизняних дослідників.

Аналіз останніх досліджень і публікацій. І. Кравець, М. Микулець, Н. Матійчук [1, с. 54] досліджували суть та складові електронного урядування. А П. Лелеченко [2] звернув увагу на ключові механізми гарантування внутрішньополітичної безпеки, націлених на скорочення та уникнення небезпек для повноцінного поступу держави відповідно до її цілей, що є складовою національних інтересів країни.

М. Дзевелюк досліджував характеристики й засади функціонування сервісної держави, а також взаємовідношення державної функції та державної послуги. [3, с. 60]. О. Пархоменко-Куцевіл [4, с. 235] запропонувала обґрунтувати й актуалізувати систему оцінювання якості надання публічних послуг та її складників.

М. А. Кутова [5, с. 20] відзначала основні аспекти інформаційної безпеки в контексті е-урядування, підкреслюючи основні виклики та розробку стратегій для підвищення ефективності захисту цифрових державних служб від магнітних загроз. Л. В. Домбровський [6] досліджував інформаційні загрози в системі національної без-

пеки. М. Ф. Криштанович [7, с. 248] визначав ключові механізми державної політики стосовно гарантування національної безпеки країни.

В. В. Любчук, Л. М. Опейда [8, с. 12] визначали риси напрямів стратегії національної безпеки як безпекового засобу державної політики. І. Г. Івасюк [9, с. 169] розглядав систему стратегій, програм, законодавчих актів та дій, спрямованих на захист інтересів держави, збереження територіальної цілісності та уникнення загроз. Автором аналізується значущість адаптації державної політики до змін в геополітичній обстановці та нових видів загроз, таких як кібернетичні атаки та збройна агресія росії.

Здійснений аналіз засвідчує, що питання електронного урядування як інструменту створення публічно-сервісної держави в умовах трансформації державної політики національної безпеки вітчизняними науковцями глибоко не досліджувалося. Наведені чинники зумовлюють актуальність обраної тематики дослідження та потребу здійснення додаткових наукових розробок.

Метою статті є визначення ролі електронного урядування у процесі становлення публічно-сервісної держави та аналіз його потенціалу як інструменту перетворення державної політики національної безпеки в умовах цифровізації та сучасних викликів.

Виклад основного матеріал. Сучасні глобальні зміни, завдяки розвитку технологій, збільшують роль знань у вирішенні проблем безпеки, що вимагає радикального дослідження державного управління. Україна, між конфліктами та гібридними війнами, також використовувала віртуальні технології для забезпечення ефективності урядової діяльності, відкритої та прозорої. У цьому контексті електронне урядування – це не лише технологічна система для вдосконалення адміністративних процедур, але й потужний інструмент в роботі державної служби, яка зосереджена на потребах громадян, обов'язків, наданні послуг тощо.

Однак, цифровізація функцій управління з часом зіткнеться з новими питаннями, особливо в національній безпеці. Розробка нової державної політики не лише забезпечує громадян, але й діє як безпека, необхідна для нестабільності суспільства цифровими каналами. Електронне урядування – це форма державного управління, засноване на широкому використанні інформаційних та комунікаційних технологій (ІКТ) для надання державних послуг та взаємодії з місцевостями, бізнесом та деякими підприємствами для підвищення прозорості, надійності та доступності процесів управління.

Основа сучасного уряду – це цифрова трансформація державної влади та місцевої влади, що вимагає не лише автоматизації процесів, але й переходу на основі культурної основи громадянина, від контролю до моделі обслуговування. Це не тільки допомагає прискорити та спростити споживання послуг, але й збільшити відповідальність уряду за забезпечення участі громадян у прийнятті рішень, що веде до покращення демократичних інститутів. Згідно з повідомленнями ООН та Європейського Союзу електронне урядування включає три ключові складові:

- G2C (Government to Citizen) – взаємодія влади з громадянами;
- G2B (Government to Business) – взаємодія з бізнесом;
- G2G (Government to Government) – взаємодія між органами влади.

У ХХІ ст. електронне урядування стало важливим фактором трансформації державного управління у всьому світі. Для України ця сфера стала особливо важливою в умовах реформ громадськості, необхідності підвищити ефективність управління та забезпечити прозорість та відповідальність уряду. У той же час, зовнішні та внутрішні виклики, особливо вторгнення росії, масові кібератаки та інформаційна війна, посилили потреби розвитку цифрової державності як фактору національної безпеки.

Починаючи з 2020 р., Україна показала значний прогрес у цифровізації послуг, особливо завдяки появі платформ «дія», розвитку інфраструктури відкритих даних та розвитку демократії. Однак, незважаючи на успіх, системні проблеми зберігаються: цифрова нерівність, фрагментація, незадовільний рівень кіберзахисту.

Цифровізація стала головним фактором, який визначає модернізацію державної системи, включаючи систему національної безпеки, яка зіткнувшись із глобальними змінами технологій та новими небезпеками, пов'язаними з цифровими технологіями, загальними підходами для забезпечення конфіденційності, виявляє те, що більше

не відповідає сучасним проблемам. Модернізація національної безпеки шляхом більш ефективної цифровізації дає змогу ефективніше реагувати на різні загрози, підвищуючи рівень інформації та захисту інфраструктури та забезпечує інтеграцію з міжнародними системами безпеки.

Цифровізація є сильним фактором модернізації системи національної безпеки, оскільки вона може значно покращити координацію державних органів влади, ефективність реакцій на надзвичайні випадки та важливий захист інфраструктури. Однак, щоб максимізувати переваги цифрових технологій, необхідно вирішити проблеми з кіберзахистом, інформаційну безпеку та цифрові знання. Успішна інтеграція цифрових рішень у національну безпеку може підвищити рівень попередження держави щодо сучасних загроз та забезпечити її стабільний розвиток.

У сучасному світі електронне урядування стало невід'ємною частиною державного управління, що може значно підвищити ефективність, прозорість та доступність державних послуг. Однак у контексті національної безпеки цей інструмент може відігравати ще важливішу роль – забезпечення стійкості громадських організацій до різних загроз. Особливо це стосується України, яка постійно стикається з зовнішніми та внутрішніми викликами, такими як вторгнення росії, кіберзагрози, інформаційна війна та внутрішні конфлікти. Відображення взаємозв'язку між електронним урядом та національною безпекою в умовах зовнішніх і внутрішніх викликів подано у табл. 3.

У сучасному світі, коли глобальні та локальні загрози робляться все більш комплексними та взаємопов'язаними, питання реформування системи безпеки та адаптація публічно-сервісної моделі держави до нових викликів набуває надзвичайно важливого значення. У цьому контексті концепція публічно-сервісної держави є одним з основних підходів для забезпечення стабільності, демократичності та ефективності управлінських процесів в умовах нової архітектури безпеки.

Нова архітектура безпеки – це пристосована концепція національної безпеки, яка враховує не тільки звичні військові загрози, але й нові виклики, такі як кіберзагрози, економічні негаразди, екологічні загрози та соціальні ризики. Це також охоплює гарантування кібербезпеки, захист критичної інфраструктури, керування кризами та розбудову суспільних інституцій, здатних оперативно реагувати на виклики. Особливості моделі публічно-сервісної держави в умовах нової архітектури безпеки подано на рис. 4.

Модель державних послуг у контексті нової архітектури безпеки повинна забезпечити баланс між ефективністю послуг та захистом національ-

ної безпеки. Цифровізація, прозорість та інтеграція передових технологій у галузі безпеки дозволяють створювати нові можливості для задоволення сучасних загроз, підвищення внутрішньої стабільності та розвитку довіри між урядом та громадянами. Успішна реалізація цієї моделі вимагає глобального підходу до адаптації до нової реальності глобальної безпеки, особливо завдяки активному використанню новітніх технологій та інтеграції державних, приватних та міжнародних сфер у систему безпеки.

У нинішньому середовищі гібридні загрози, кібератаки та збільшення важливості інформаційних технологій у державній діяльності, електронне урядування стає важливим фактором не лише ефективного управління, але й національної безпеки. Інструменти, послуги та цифрові платформи, що використовуються в державному управлінні, мають великий потенціал для підвищення стабільності країни до внутрішніх та зовнішніх загроз. У той же час їх реалізація вимагає стратегічного підходу, чіткої координації між органами влади та інтегрується в загальну систему політики безпеки.

Україна, що вже має досвід створення цифрових сервісів через проекти як-от «Дія», постає перед задачею – поєднати здобутки цифрової

трансформації з реальними механізмами гарантування безпеки. Це включає не тільки захист державних ІТ-систем, а й побудову довіри до електронного урядування, забезпечення прозорості, оперативності реагування на загрози та цифрової грамотності громадян.

Практичні рекомендації щодо інтеграції електронного урядування в державну політику безпеки України подано у табл. 6.

Інтеграція електронного урядування в державну політику безпеки України є стратегічним пріоритетом, що сприяє розбудові сучасної, ефективної та стійкої системи публічної влади. Запропоновані поради обґрунтовують потребу комплексного підходу до цифрової трансформації безпекового сектору; цей підхід передбачає поєднання технологічного прогресу, нормативно-правового забезпечення, кадрової модернізації та міжвідомчої координації.

Реалізація цих заходів не тільки підвищить кібербезпеку та захистить важливу інфраструктуру держави, але й сприятиме громадській довірі у цифрових державних послугах, що оптимізує їхні процеси управління та забезпечить їх прозорість. Електронне урядування не тільки виконує функцію постачальника послуг, але й стає основним елементом нової моделі державної безпеки.

Таблиця 3

Взаємозв'язок між електронним урядуванням та національною безпекою в умовах зовнішніх і внутрішніх викликів

Критерії	Роль електронного урядування	Зовнішні виклики	Внутрішні виклики
Кібербезпека	Забезпечення оборони від кіберзагроз через використання надійних цифрових майданчиків.	Кібератаки з боку агресора, зокрема на важливу інфраструктуру (енергетичні мережі, військові частини)	Необхідність у посиленні внутрішньої кібербезпеки, створення дієвих заходів для захисту особистих даних громадян
Інформаційна безпека	Захист від інформаційних нападів, фальшувань та маніпуляцій у медіа і в Інтернеті	Військові та гібридні напади через дезінформацію, пропаганду, намагання впливати на суспільну думку в умовах війни.	Внутрішні інформаційні небезпеки, такі як пропаганда в засобах масової інформації, поширення неправдивих відомостей серед людей
Ефективність управління	Оперативне керування через електронні платформи, швидке ухвалення рішень.	Оперативна відповідь на зовнішні кризи, особливо під час війни чи стихійних лих, через інтеграцію державних баз даних.	Ризики політичної нестабільності, корупційні виклики, недовіра до інституцій влади через непрозорість процедур управління
Захист критичної інфраструктури	Цифрові системи для спостереження та управління важливими ресурсами	Атаки на критичну інфраструктуру (енергетичні мережі, транспорт, комунікації)	Потреба в обороні національних ресурсів, інфраструктури від внутрішніх небезпек, таких як диверсії або саботаж.
Залучення громадян до управління	Платформи для електронної демократії, зокрема петиції, опитування, електронне голосування	Використання цифрових платформ задля взаємодії з громадянами, враховуючи збір та аналіз громадської думки в час криз	Зміцнення довіри до країни через прозорість та доступність цифрових сервісів для громадян, зокрема у віддалених областях

Джерело: сформовано автором на основі [10, с. 68].

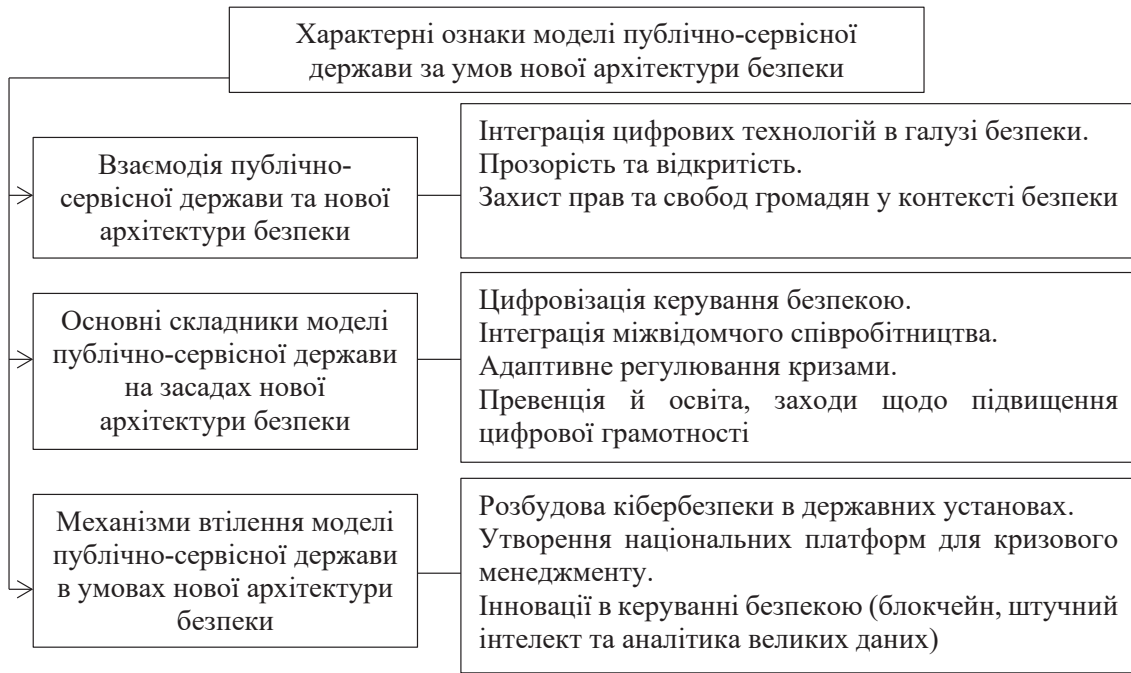


Рис. 4. Особливості моделі публічно-сервісної держави в умовах нової архітектури безпеки

Джерело: сформовано автором на основі [11, с. 155].

Таблиця 6

Напрямки інтеграції електронного урядування в державну політику безпеки України

Напрямки	Мета	Інструменти	Очікуваний результат
Єдина цифрова платформа для безпечності	Централізація збирання, опрацювання та обміну відомостями про небезпеки	створення Національного центру цифрової безпеки на основі вже наявних платформ (як-от, Дія)	Оперативність відповіді, зменшення повторення функцій між органами
Цифрова ідентифікація в охоронних сервісах	Унеможливити нелегальний доступ до захищених державних ресурсів	біометричні паспорти, BankID, MobileID, цифрові підписи	Підвищення рівня довіри до електронних сервісів та зниження кіберзагроз
Міжвідомча цифрова інтеграція	Забезпечити дієву координацію між МВС, СБУ, Держспецзв'язком, Міноборони тощо.	Спільні бази даних, інтегровані системи інформаційної безпеки	Швидке виявлення небезпек та узгодженість операцій
Нормативне закріплення цифрових засобів у політиці	Включити електронне врядування до основних документів державної політики національної безпеки	Внесення змін до Стратегії національної безпеки, Концепції кібербезпеки	Чітке нормативне визначення та фінансова підтримка цифрових починань у галузі безпеки
Аудит цифрової інфраструктури	Виявити вразливі місця в IT-системах державних інституцій	Регулярні випробування на проникнення, аудит коду, оцінка ступеня шифрування даних	Зменшення ризику кіберінцидентів
Постійне навчання держслужбовців	Підвищити професійність держслужбовців щодо цифрових загроз	Онлайн-курси, імітаційні навчання, атестації	Зменшення людського чинника як джерела вразливостей
Державно-приватне партнерство в IT-безпеці	Залучити технологічні фірми до спільного протидії загрозам	Укладання договорів про співпрацю, пілотні плани, інкубатори безпекових технологій	Використання найліпших світових практик та нововведень
Прозорість і довіра до е-сервісів безпеки	Уникнути маніпулювання та дезінформації	Публічні звіти про застосування даних, механізми нагляду та зворотного зв'язку	Зміцнення правомірності державної політики безпеки

Джерело: сформовано та доповнено автором на основі [12, с. 49].

Тому реальність цих рекомендацій стає необхідною умовою для становлення цифрової, орієнтованої на суспільне благо України.

Висновки. У процесі реформування державної політики у сфері національної безпеки електронне урядування виступає як ключовий інструмент модернізації публічного управління. Його інтеграція не тільки сприяє покращенню якості та досяжності державних послуг, але й гарантує прозорість, підзвітність і відкритість влади – основні риси сервісно-орієнтованої держави.

Електронне урядування змінило модель взаємодії між державою та суспільством: зосередження уваги на адміністративному контролі над наданням послуг, мобілізації громадян за допомогою цифрових інструментів для участі в управлінських рішеннях та полегшення довіри до громадських організацій. У цьому контексті цифровізація не тільки вважається технологічним процесом, але й стратегічним фактором для забезпечення стабільності, адаптивності та безпеки держави. Пріоритетні компоненти політики національної безпеки повинні розробляти цифрові рішення в галузі безпеки,

захист важливої інформаційної інфраструктури, підвищення рівня кіберзахисту, а також створення необхідних юридичних умов та організації, необхідних для здійснення цифрових змін.

Отже, електронне урядування постає не тільки механізмом раціоналізації адміністративних процесів, але й відіграє вкрай важливу роль у забезпеченні архітектури національної безпеки. Його впровадження до системи державного управління мусить відбуватися системно, з дотриманням балансу між інституційними й технічними рівнями. Це сприятиме підтримці демократичних процесів та зміцненню спроможності держави протидіяти сучасним викликам.

Перспективними напрямками майбутніх наукових розвідок можуть стати проекти з моделювання синергії між електронним урядуванням та секторами державної безпеки. Особливий інтерес викликає розробка інтегрованих цифрових рішень задля координації діяльності правоохоронних органів, оборонних структур, кризових служб і галузі цивільного захисту в рамках єдиної системи управління загрозами.

REFERENCES:

1. Kravets I., Mykulets M., & Matiichuk N. (2024). Elektronne uriaduvannya yak instrument zabezpechennia balansu interesiv hromadian i derzhavy [E-governance as a tool for balancing the interests of citizens and the state]. *Herald of Khmelnytskyi National University. Economic Sciences*, 330(3), 54-58. DOI: <https://doi.org/10.31891/2307-5740-2024-330-7>.
2. Lelechenko A. (2022). Mechanisms for ensuring internal political security in conditions of democratization of civil society. *Derzhavne upravlinnya: udoskonalennya ta rozvytok*, 3. DOI: 10.32702/2307-2156-2022.3.1.
3. Dzeveluk M. V. (2017). Servisna derzhava yak funktsionalna model suchasnoi derzhavy [The service state as a functional model of the modern state]. *Aktualni problemy derzhavy i prava: zb. nauk. Pr.*, 78, 60-67. available at: <https://dspace.onua.edu.ua/server/api/core/bitstreams/b82343b5-5274-4a1b-a911-237fdd29bb11/content>.
4. Parkhomenko-Kutsevil O. (2024). Zaprovaldzhennia tsyfrovizatsii u protses zabezpechennia yakosti publichnykh posluh [Introducing digitalization into the process of ensuring the quality of public services]. *Naukovi innovatsii ta peredovi tekhnolohii*, 2 (30), 235-245. DOI: [https://doi.org/10.52058/2786-5274-2024-2\(30\)-235-245](https://doi.org/10.52058/2786-5274-2024-2(30)-235-245).
5. Kutova M. A. (2024). Osnovy informatsiinoi bezpeky v systemi elektronnoho uriaduvannya [Basics of information security in the e-government system]. *Economic Synergy*, 1, 20-30. available at: <https://doi.org/10.53920/ES-2024-1-2>.
6. Dombrovskiy 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*. available at: <http://repositc.nuczu.edu.ua/bitstream/123456789/20339/1/12Dombrovskiy.pdf>.
7. Kryshchanovych M. F. (2019). Mekhanizmy derzhavnoi polityky Ukrainy shchodo zabezpechennia natsionalnoi bezpeky [Mechanisms of the State Policy of Ukraine to Ensure National Security]. *Publichne upravlinnia ta mytne administruvannya*, 3 (22), 248-253. DOI <https://doi.org/10.32836/2310-9653-2019-3-248-253>.
8. Liubchuk V. V., & Opeida L. M. (2024). Stratehiia natsionalnoi bezpeky Ukrainy yak bezpekovi instrument derzhavnoi polityky [National Security Strategy of Ukraine as a Security Instrument of the State Policy]. *Acta securitatis volyniensis*, 3, 12-16. DOI <https://doi.org/10.32782/2786-9385/2024-3-2>.
9. Ivasiuk I. H. (2024). Zahalna kharakterystyka derzhavnoi polityky u sferi natsionalnoi bezpeky Ukrainy [General characteristics of the state policy in the field of national security of Ukraine]. *Aktualni problemy vitchyzniansoi yurysprudentsii*, 1, 169-174. DOI <https://doi.org/10.32782/2408-9257-2024-1-31>.
10. Kondratieva, K. A. (2024). Znachennia pravovoho rehuliuвання e-vriaduvannya dlia natsionalnoi bezpeky Ukrainy v umovakh voiennoho stanu [The Importance of Legal Regulation of E-Governance for the National Security of Ukraine in the Context of Martial Law]. *Visnyk studentskoho naukovoho tovarystva DonNU imeni Vasyliia Stusa*, 16(2), 68-72. available at: <https://jvestnik-sss.donnu.edu.ua/article/view/16839>.
11. Slobodeniuk T. O. (2024). Perspektyvna model publichno-servisnoi derzhavy v Ukraini [A promising model of a public service state in Ukraine]. *Investysii: praktyka ta dosvid*, 18, 155-160. DOI: 10.32702/2306-6814.2024.18.155.
12. Yusifbeili R. (2021). Stratehichni napriamy rozvytku elektronnoho uriaduvannya v Ukraini [Strategic directions of e-government development in Ukraine]. *Publichne upravlinnia ta mytne administruvannya*, 2 (29), 49-55. DOI <https://doi.org/10.32836/2310-9653-2021-2-8>.