

<https://doi.org/10.31891/2307-5740-2025-340-8>

УДК: 351.746.1:004.056

КУТОВА Марина

Національний університет «Чернігівська політехніка»

<https://orcid.org/0009-0007-1693-7278>e-mail: [dekfmip@gmail.com](mailto:dekfmip@gmail.com)

## ІДЕНТИФІКАЦІЯ СТРАТЕГІЧНИХ НАПРЯМІВ РОЗВИТКУ СИСТЕМИ ЕЛЕКТРОННОГО УРЯДУВАННЯ В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті визначено стратегічні напрями розвитку системи електронного урядування в Україні з урахуванням аспектів інформаційної безпеки. Доведено, що сучасні інформаційні технології забезпечують відкритість, прозорість та ефективність державного управління, але водночас породжують нові кіберзагрози. Проаналізовано нормативно-правову базу, інституційну структуру, технологічні аспекти, цифрову грамотність та міжнародну співпрацю як ключові компоненти системи забезпечення інформаційної безпеки. Визначено, що подальший розвиток електронного урядування вимагає системного підходу та інтеграції принципів кібербезпеки у процес державного управління.

Ключові слова: електронне урядування, інформаційна безпека, кібербезпека, стратегічні напрями, цифровізація, нормативно-правова база.

KUTOVA Maryna

Chernihiv Polytechnic National University

## IDENTIFICATION OF STRATEGIC DIRECTIONS FOR THE DEVELOPMENT OF THE E-GOVERNANCE SYSTEM IN THE CONTEXT OF INFORMATION SECURITY

The article identifies strategic directions for developing Ukraine's e-governance system, emphasizing information security aspects. The author notes that the development of information society significantly transforms traditional approaches to public administration. E-governance acts as a critical tool that ensures transparency, efficiency, and responsiveness of public administration processes. However, the adoption of advanced information and communication technologies (ICT) simultaneously generates new cybersecurity challenges.

The research analyzes the existing regulatory and legal framework, institutional structure, technological dimensions, digital literacy initiatives, and international collaboration efforts, highlighting their importance in building a robust information security ecosystem. The regulatory environment requires continuous updating and flexibility due to rapid technological advances and evolving cyber threats. Institutional modernization, particularly the creation of specialized cybersecurity units like CERT-UA and cybersecurity departments within the Ministry of Digital Transformation, significantly enhances the state's capabilities to address cyber threats effectively.

Technological advancements enable rapid monitoring, threat detection, and innovative security management but also create dependencies on providers and risks related to software vulnerabilities. Digital literacy initiatives are essential for minimizing human-factor-related cyber threats, although their effectiveness demands a comprehensive and sustained educational approach. Finally, international cooperation is pivotal in sharing best practices and standards, despite challenges posed by political differences and varying state interests.

The article concludes that future e-governance development in Ukraine should integrate a comprehensive, strategic approach emphasizing cybersecurity as an integral component of public administration.

Keywords: e-governance, information security, cybersecurity, strategic directions, digitalization, regulatory framework.

### ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Розвиток інформаційного суспільства суттєво впливає на формування нових підходів до управління державою, актуалізуючи застосування сучасних інформаційних технологій у публічному управлінні. Електронне урядування виступає ключовим інструментом у забезпеченні прозорості, ефективності та оперативності державного управління, але разом із цим воно породжує нові виклики у сфері інформаційної безпеки, що вимагає відповідної адаптації системи державного управління та розвитку стратегічних напрямів електронного урядування з акцентом на безпеку інформації.

### АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Питання розвитку електронного урядування широко розглядаються у працях українських та зарубіжних дослідників. Електронне урядування розглядається як сучасна форма організації державного управління, яка завдяки активному використанню новітніх інформаційно-комунікаційних технологій значно покращує взаємодію держави із суспільством. Воно сприяє підвищенню прозорості, відкритості та доступності державних послуг, дозволяючи надавати комплекс послуг як громадянам, так і бізнесу. Такий підхід дозволяє зменшити бюрократичні перешкоди, оптимізувати адміністративні процеси та суттєво покращити якість обслуговування населення [1, 2, 4, 5]. Зокрема, дослідники Азарова А.О., Ткачук Л.М. та Нікіфорова Л.О. визначають, що ефективне електронне урядування є ключовим чинником підвищення ефективності публічного управління, а також сприяє зростанню рівня довіри до державних інституцій з боку громадян та бізнес-середовища [1, 5]. Подібні висновки представлені й у працях Гайдученко С.О.,

наголошуючи, що електронне урядування дозволяє впроваджувати новітні стандарти адміністративної діяльності, а також забезпечує зручний і швидкий доступ громадян до необхідних їм послуг [2].

Особлива увага в наукових працях приділяється питанню забезпечення кібербезпеки як необхідної умови ефективного розвитку електронного урядування. Кібербезпека розглядається як динамічний процес, який потребує постійного оновлення та адаптації до нових викликів. Це пов'язано із швидким розвитком кіберзагроз та появою нових методів їх нейтралізації. Так, за результатами досліджень Котух Є.В., забезпечення кібербезпеки в публічному секторі передбачає створення комплексної системи заходів, яка включає моніторинг загроз, оцінку ризиків та впровадження ефективних заходів протидії, які здатні оперативно реагувати на будь-які зміни кіберзагроз [3]. У працях Баранова О.А., Демкової М.С. та Дзюби С.В. акцентовано увагу на концептуальних засадах розвитку електронного урядування, де наголошується, що ефективність електронного урядування безпосередньо залежить від наявності належної нормативно-правової бази та підтримки з боку органів державної влади [4].

Аналіз праць різних авторів дозволяє зробити висновок, що подальший розвиток електронного урядування в Україні має здійснюватися з урахуванням сучасних викликів, зокрема, у сфері кібербезпеки, а також на основі чіткого розуміння ролі і значення новітніх інформаційних технологій для забезпечення відкритої та ефективної взаємодії державних органів із суспільством [1, 2, 3, 4, 5].

### **ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ**

Попри значну кількість досліджень у сфері електронного урядування, недостатньо розробленими залишаються стратегічні напрями, орієнтовані на забезпечення інформаційної безпеки в контексті зростаючих кіберзагроз. Недостатньо вивчено механізми стратегічної інтеграції принципів кібербезпеки у процес розвитку електронного урядування.

### **ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ**

Метою статті є визначення стратегічних напрямів розвитку електронного урядування в Україні з акцентом на забезпечення інформаційної безпеки.

### **ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ**

Розвиток електронного урядування в Україні передбачає стратегічний підхід, що враховує комплексний аналіз викликів у сфері інформаційної безпеки. В умовах цифровізації суспільства, коли обсяги інформації невпинно зростають, питання захисту інформації стає критичним завданням для державних органів влади. Це зумовлено як постійним розвитком інформаційно-комунікаційних технологій, так і збільшенням кількості та складності кіберзагроз, які набувають дедалі витонченішого характеру. Зростання обсягів даних, що циркулюють в інформаційних системах державного сектора, створює умови для потенційних втрат, витоків інформації та несанкціонованого доступу. Ключовим стратегічним напрямом забезпечення інформаційної безпеки є формування та постійне вдосконалення нормативно-правової бази [6,7,8,9] (рис.1).

Україна вже досягла певного прогресу, створивши основні законодавчі акти, що регламентують питання інформаційної безпеки [6,7,8]. Водночас, сучасна практика демонструє необхідність регулярного оновлення цієї нормативної бази для адекватної відповіді на нові виклики цифрової епохи [9]. Перевагою цього підходу є формування чітких процедур і стандартів, що дозволяють державним органам ефективно діяти в умовах кіберкриз. Втім, очевидними недоліками залишаються високі темпи старіння правових норм через швидку зміну технологій і методів кіберзлочинців. Таким чином, законодавча база повинна бути достатньо гнучкою та орієнтованою на швидке реагування на нові загрози.

Другим стратегічним напрямом є інституційна модернізація державних органів, які відповідають за кібербезпеку [10,11]. Сьогодні вже створюються спеціалізовані структури, такі як CERT-UA [10] та підрозділи кібербезпеки у Міністерстві цифрової трансформації [11], які здатні швидко реагувати на виникнення загроз. Основною перевагою такого підходу є оперативність та ефективна координація дій різних державних органів. Однак цей процес супроводжується значними фінансовими витратами та дефіцитом кваліфікованих кадрів у сфері кібербезпеки. Проблема підготовки фахівців є критичною, адже без належного кадрового забезпечення навіть найкращі структури не зможуть повноцінно виконувати свої функції. Тому необхідно впроваджувати комплексні програми кадрової підготовки та підвищення кваліфікації.

Третій напрям стратегії розвитку електронного урядування - це використання новітніх інформаційних технологій та сучасних програмних продуктів для забезпечення інформаційної безпеки. Такі рішення дозволяють автоматизувати процеси моніторингу, оперативного реагування на загрози, а також впроваджувати інноваційні методи захисту інформації. Переваги цього підходу очевидні: він забезпечує високу адаптивність систем до нових загроз, швидке оновлення та інтеграцію новітніх досягнень у сфері інформаційної безпеки. Проте разом з перевагами виникають і ризики - програмні збої, помилки у реалізації, кіберінциденти через недоліки в програмному коді, а також надмірна залежність від технологічних партнерів

та постачальників послуг. Тому важливо ретельно проводити аудит технологій, оцінювати потенційні ризики та обирати надійних партнерів.



Рис. 1. Стратегічні напрями розвитку електронного урядування в контексті забезпечення інформаційної безпеки  
Джерело: побудовано автором на основі [5,10,11]

Четвертий стратегічний напрям - це розвиток цифрової грамотності населення та державних службовців. Особливо важливим цей напрям стає з огляду на те, що значна частина кіберзагроз пов'язана саме з людським фактором: необережністю, недостатньою увагою, низьким рівнем кібергігієни. Впровадження освітніх програм і тренінгів у цій сфері дозволяє суттєво знизити ризики, які пов'язані з несанкціонованим доступом та витоком інформації через людський фактор. Проте, як свідчить практика, цей процес потребує значного часу та систематичного підходу. Важливо забезпечити доступ до освіти різним соціальним групам, включаючи вразливі категорії громадян.

П'ятий стратегічний напрям - міжнародна співпраця. Враховуючи глобальний характер кіберпростору, національна інформаційна безпека не може бути ефективною без взаємодії з міжнародними партнерами. Україна активно співпрацює з міжнародними структурами, такими як НАТО, ЄС, ОБСЄ, в рамках яких реалізуються спільні проекти, навчання, обмін досвідом та найкращими практиками. Перевагою цієї взаємодії є доступ до провідних технологій, стандартів і методик протидії кіберзагрозам. Проте і тут виникають ризики, пов'язані з політичними розбіжностями, конфліктом інтересів держав-партнерів та складністю досягнення консенсусу з багатьох принципових питань.

Таким чином, стратегічний розвиток електронного урядування в Україні має базуватися на комплексному підході, який поєднує вдосконалення законодавства, модернізацію державних структур, технологічні інновації, підвищення цифрової грамотності та міжнародну співпрацю. Лише цілісне застосування всіх цих напрямів дозволить Україні ефективно захищати свою інформацію у кіберпросторі.

### ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У результаті проведеного дослідження визначено, що розвиток електронного урядування в Україні має базуватися на комплексному стратегічному підході. Основними складовими цього підходу є

вдосконалення нормативно-правової бази, модернізація інституційної структури, впровадження сучасних технологічних рішень, підвищення цифрової грамотності громадян та активізація міжнародного співробітництва у сфері кібербезпеки. Доведено, що ефективне електронне урядування можливе лише за умови інтеграції та пріоритетного врахування аспектів інформаційної безпеки. Встановлено, що найуразливішими аспектами залишаються нормативно-правова база та кадрове забезпечення кібербезпеки, що потребують постійного оновлення та системної підготовки фахівців. Наголошено на важливості розвитку цифрових компетенцій населення для мінімізації ризиків людського фактору.

Перспективними напрямками подальших досліджень є поглиблене вивчення механізмів міжнародного співробітництва та створення адаптивних моделей нормативно-правового регулювання у сфері інформаційної безпеки. Особливої уваги заслуговують розробки ефективних освітніх програм для підвищення цифрової грамотності громадян та державних службовців. Також актуальними є дослідження впливу нових інформаційних технологій на ефективність публічного управління з позицій забезпечення кібербезпеки.

### Література

1. Азарова А.О. Публічне управління та адміністрування : навчальний посібник / А.О. Азарова, Л.М. Ткачук, Л.О. Нікіфорова та ін. Вінниця : ВНТУ, 2019. 181 с.
2. Гайдученко С.О. Електронне урядування : конспект лекцій для студентів усіх форм навчання спеціальності 281 – Публічне управління та адміністрування. Харків : ХНУМГ ім. О.М. Бекетова, 2019. 54 с.
3. Котух Є.В. Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі : дис. ... д-ра наук з держ. упр. : 25.00.02 «Механізми державного управління». Харків, 2022. 512 с.
4. Концептуальні засади розвитку електронного урядування в Україні/О.А. Баранов, М.С. Демкова, С.В. Дзюба та ін.; за ред. А.І. Семенченко. Київ, 2009. 82 с.
5. Ткачук Л.М. Підвищення ефективності публічного управління засобами електронного урядування / Л.М. Ткачук, О.А. Стахова // Modern Technologies and Prospects of Economic Development. 2020. С. 167–175. DOI: <https://doi.org/10.30525/978-9934-588-66-2-10>.
6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (дата звернення: 02.03.2025).
7. Про Національну програму інформатизації : Закон України від 04.02.1998 № 74/98-ВР. URL: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80> (дата звернення: 02.03.2025).
8. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15> (дата звернення: 02.03.2025).
9. Стан нормативно-правового регулювання інформаційної безпеки в Україні. Офіційний портал Верховної Ради України. URL: [https://kno.rada.gov.ua/news/Inform-analit\\_mat/VI\\_skl/73589.html](https://kno.rada.gov.ua/news/Inform-analit_mat/VI_skl/73589.html) (дата звернення: 02.03.2025).
10. Діяльність Державного центру кіберзахисту CERT-UA. Офіційний сайт Держспецзв'язку. URL: <https://cert.gov.ua> (дата звернення: 02.03.2025).
11. Міністерство цифрової трансформації України. Офіційний сайт. URL: <https://thedigital.gov.ua> (дата звернення: 02.03.2025).

### References

1. Azarova A.O. Public Administration and Governance: textbook / A.O. Azarova, L.M. Tkachuk, L.O. Nikiforova et al. Vinnytsia: VNTU, 2019. 181 p.
2. Haiduchenko S.O. E-Government: lecture notes for students of all forms of study in the specialty 281 – Public Administration and Governance. Kharkiv: KhNUMG named after O.M. Beketov, 2019. 54 p.
3. Kotukh Ye.V. Theoretical and Methodological Foundations of Cybersecurity in the Public Sector: doctoral dissertation in public administration: 25.00.02 "Mechanisms of Public Administration". Kharkiv, 2022. 512 p.
4. Conceptual Foundations for the Development of E-Government in Ukraine / O.A. Baranov, M.S. Demkova, S.V. Dziuba et al.; edited by A.I. Semenchko. Kyiv, 2009. 82 p.
5. Tkachuk L.M. Improving the Efficiency of Public Administration through E-Government Tools / L.M. Tkachuk, O.A. Stakhova // Modern Technologies and Prospects of Economic Development. 2020. pp. 167–175. DOI: <https://doi.org/10.30525/978-9934-588-66-2-10>.
6. On Information Protection in Information and Telecommunication Systems: Law of Ukraine dated 05.07.1994 No. 80/94-VR. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80> (accessed: 02.03.2025).
7. On the National Informatization Program: Law of Ukraine dated 04.02.1998 No. 74/98-VR. URL: <https://zakon.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80> (accessed: 02.03.2025).
8. On Electronic Documents and Electronic Document Management: Law of Ukraine dated 22.05.2003 No. 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15> (accessed: 02.03.2025).
9. The State of Regulatory and Legal Framework for Information Security in Ukraine. Official portal of the Verkhovna Rada of Ukraine. URL: [https://kno.rada.gov.ua/news/Inform-analit\\_mat/VI\\_skl/73589.html](https://kno.rada.gov.ua/news/Inform-analit_mat/VI_skl/73589.html) (accessed: 02.03.2025).
10. Activities of the State Cyber Protection Center CERT-UA. Official website of the State Special Communications Service. URL: <https://cert.gov.ua> (accessed: 02.03.2025).
11. Ministry of Digital Transformation of Ukraine. Official website. URL: <https://thedigital.gov.ua> (accessed: 02.03.2025).