International Experience of Digitization of Activities of State Authorities

UDC: 351:004.77 DOI: https://doi.org/10.15421/152443

Bermas Andrii
Ph.D. Student, https://orcid.org/0009-0005-8823-9685, andriybermas@gmail.com
Odesa I. I. Mechnykov National University (Odesa,Ukraine)

Abstract

Relevance. The need to systematise and comprehensively analyse the existing risks and threats to the digital transformation of public authorities is driven by the need to develop effective strategies to overcome them, but also to create conditions for ensuring the sustainable, safe and efficient functioning of public institutions in the digital environment. The study takes into account technological, socio-economic, organisational and legal factors, given the need to create a comprehensive strategy that will ensure the security, efficiency and transparency of public authorities in the digital age, especially in the context of Ukraine's European integration aspirations.

The purpose. Comprehensive identification of risks, threats and vulnerabilities associated with digital transformation in Ukrainian public authorities, followed by the development of practical recommendations for their neutralisation.

Results. A number of significant gaps in the legal regulation of digitalisation processes in Ukraine have been identified, which impede the effective implementation of the digital transformation of public administration and create additional risks. The main aspects that require attention include legislative inconsistencies, insufficient regulation in the field of cybersecurity and the lack of clear mechanisms for protecting the rights of citizens in the digital space.

Conclusions. The digital modernisation of public administration is an inevitable process that opens up broad prospects for increasing the efficiency, transparency and accessibility of public services. However, this process is accompanied by significant challenges related to information security, risk management and countering cyber threats. The results of the study confirm that successful implementation of digital transformation in public authorities requires a systematic approach that covers technical, organisational and human aspects.

Keywords: digital transformation, authorities, risks of digitalisation, cybersecurity, digital competences, e-government, information security, modernisation, public administration, digitalisation, cyber threats

Міжнародний досвід діджиталізації діяльності органів державної влади

Бермас Андрій
Одеський національний університет імені І. І. Мечникова (Одеса, Україна)

Анотація

Актуальність дослідження: Потреба систематизації та всебічного аналізу наявних ризиків і загроз цифрової трансформації органів державної влади зумовлена необхідністю розробки результативних стратегій їх подолання , але й створенням умов для забезпечення стійкого, безпечного та ефективного функціонування державних інституцій у цифровому середовищі. Дослідження враховує технологічні, соціально-економічні, організаційні та правові фактори, враховуючи необхідність створення цілісної стратегії, яка забезпечить безпеку, ефективність і прозорість функціонування органів державної влади в умовах цифрової епохи, особливо в контексті євроінтеграційних прагнень України.

Мета дослідження: Комплексне визначення ризиків, загроз та вразливостей, які пов'язані із цифровою трансформацією в органах державної влади України з подальшою розробкою практичних рекомендацій щодо їх нейтралізації.

Результати дослідження: Виявлено низку суттєвих прогалин у правовому регулюванні процесів цифровізації в Україні, які гальмують ефективну реалізацію цифрової трансформації державного управління та створюють додаткові ризики. Основні аспекти, що потребують уваги, включають законодавчі неузгодженості, недостатнє регулювання у сфері кібербезпеки та відсутність чітких механізмів захисту прав громадян у цифровому просторі.

Висновки. Цифрова модернізація державного управління є невідворотним процесом, що відкриває широкі перспективи для підвищення ефективності, прозорості та доступності державних послуг. Однак цей процес супроводжується значними викликами, пов'язаними із забезпеченням інформаційної безпеки, управлінням ризиками та протидією кіберзагрозам. Результати дослідження підтверджують, що для успішної реалізації цифрової трансформації в органах державної влади необхідний системний підхід, який охоплює технічні, організаційні та людські аспекти.

Ключові слова: цифрова трансформація, органи влади, ризики цифровізації, кібербезпека, цифрові компетенції, електронне урядування, інформаційна безпека, модернізація, державне управління, діджиталізація, кіберзагрози

Стаття надійшла / Article arrived: 19.10.2024 Схвалено до друку / Accepted: 12.12.2024

Вступ.

Діджиталізація державного управління є невід'ємною частиною сучасного розвитку України та світу загалом. Цей процес передбачає впровадження цифрових технологій у діяльність органів державної влади з метою підвищення ефективності їх функціонування та якості надання послуг громадянам. Однак, поряд із численними перевагами, діджиталізація несе в собі певні ризики та загрози, які потребують ретельного вивчення та розробки механізмів їх подолання (Карпенко, 2020, с. 12).

У контексті державного управління діджиталізація розглядається як "процес впровадження цифрових технологій для оптимізації та автоматизації робочих процесів, покращення комунікації між державними органами та громадянами, а також підвищення прозорості та підзвітності влади (Куйбіда, 2018, с. 45). Це визначення підкреслює комплексний характер діджиталізації та її вплив на різні аспекти діяльності органів державної влади.

Актуальність дослідження ризиків та загроз діджиталізації в органах державної влади зумовлена стрімким розвитком інформаційно-комунікаційних технологій та їх активним впровадженням у сферу державного управління. Розуміння потенційних небезпек дозволить розробити ефективні стратегії захисту та мінімізації негативних наслідків цифрової трансформації.

Метою даного дослідження є розгляд основних ризиків та загроз, пов'язаних з діджиталізацією діяльності органів державної влади, а також визначення можливих шляхів їх подолання. Особлива увага приділяється питанням інформаційної безпеки, захисту персональних даних, кібербезпеки та соціально-економічних наслідків цифрової трансформації.

У рамках дослідження розглядаються як технічні аспекти ризиків діджиталізації, так і їх вплив на організаційну структуру, кадрову політику та процеси прийняття рішень в органах державної влади. Важливим аспектом є також аналіз правового регулювання процесів діджиталізації та визначення прогалин у законодавстві, які можуть створювати додаткові загрози.

Практична значущість даного дослідження полягає у формуванні комплексного підходу до оцінки та управління ризиками діджиталізації в органах державної влади. Результати роботи можуть бути використані при розробці стратегій цифрової трансформації, вдосконаленні нормативно-правової бази та створенні систем захисту від кіберзагроз.

Структура дослідження включає аналіз попередніх досліджень і публікацій, детальний розгляд результатів дослідження та формулювання висновків. Такий підхід дозволяє всебічно розглянути проблему ризиків та загроз діджиталізації в органах державної влади та запропонувати обґрунтовані рекомендації щодо їх мінімізації.

Аналіз попередніх досліджень і публікацій. Проблематика ризиків та загроз діджиталізації в органах державної влади привертає увагу багатьох українських дослідників. Значний внесок у розвиток цього напряму зробили такі вчені, як О. В. Карпенко, В. С. Куйбіда, О. В. Орлов, М. С. Міхровська та інші. Їхні праці створюють теоретичне підґрунтя для подальших досліджень у цій сфері (Орлов, 2019, с. 78).

О. В. Карпенко у своїх роботах акцентує увагу на інформаційній безпеці як ключовому аспекті діджиталізації державного управління. Він наголошує на необхідності створення комплексної системи захисту інформації в органах державної влади, яка б враховувала як технічні, так і організаційні аспекти безпеки (Карпенко, 2021, с. 23).

В. С. Куйбіда розглядає ризики діджиталізації в контексті трансформації системи державного управління. Він підкреслює важливість адаптації організаційної структури та процесів прийняття рішень до нових умов цифрового середовища. Особливу увагу дослідник приділяє питанням підготовки кадрів та розвитку цифрових компетенцій державних службовців (Куйбіда, 2019, с. 56).

О. В. Орлов фокусується на правових аспектах діджиталізації та пов'язаних з ними ризиках. Він аналізує існуючу нормативно-правову базу та виявляє прогалини, які можуть створювати загрози для ефективного функціонування електронного урядування. Дослідник пропонує шляхи вдосконалення законодавства з метою мінімізації правових ризиків (Орлов, 2020, с. 34).

М. С. Міхровська досліджує соціально-економічні наслідки діджиталізації органів державної влади. Вона звертає увагу на потенційні ризики, пов'язані зі зміною структури зайнятості, цифровою нерівністю та необхідністю адаптації громадян до нових форм взаємодії з державними органами (Міхровська, 2021, с. 89).

Важливим аспектом, який розглядається у попередніх дослідженнях, є кібербезпека органів державної влади. Зокрема, В. Ю. Степанов аналізує сучасні кіберзагрози та пропонує методи їх нейтралізації в контексті діджиталізації державного управління. Він наголошує на необхідності створення ефективної системи

кіберзахисту, яка б враховувала специфіку діяльності органів державної влади (Степанов, 2020, с. 67).

Аналіз попередніх досліджень і публікацій демонструє багатогранність проблеми ризиків та загроз діджиталізації в органах державної влади. Водночас, існує потреба в подальшому вивченні цієї теми, особливо в контексті стрімкого розвитку технологій та змін у глобальному інформаційному середовищі.

Результати дослідження.

Аналіз ризиків та загроз діджиталізації в органах державної влади дозволив виявити ряд ключових проблем, які потребують особливої уваги. Перш за все, варто відзначити загрози інформаційній безпеці, які набувають особливої актуальності в умовах цифрової трансформації. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кібератак на державні інформаційні ресурси зросла на 35% у 2023 році порівняно з попереднім роком (Державна служба спеціального зв'язку та захисту інформації України, 2024, с. 12). Це свідчить про необхідність посилення заходів захисту та вдосконалення систем кібербезпеки в органах державної влади.ґ

Одним із найбільш серйозних ризиків є можливість несанкціонованого доступу до конфіденційної інформації та персональних даних громадян. У цьому контексті важливо звернути увагу на визначення поняття "захист персональних даних" як "комплексу правових, організаційних та технічних заходів, спрямованих на забезпечення недоторканності персональних даних та їх захист від несанкціонованого доступу, знищення, модифікації, блокування, копіювання, поширення, а також інших неправомірних дій" (Золотар, 2022, с. 78). Забезпечення належного рівня захисту персональних даних є критичним завданням для органів державної влади в процесі діджиталізації.

Дослідження виявило, що значну загрозу становить також недостатній рівень цифрової грамотності як серед державних службовців, так і серед громадян. За даними Міністерства цифрової трансформації України, лише 53% українців володіють базовими цифровими навичками (Міністерство цифрової трансформації України, 2023, с. 45). Це створює ризики неефективного використання цифрових інструментів, помилок при роботі з даними та вразливості до соціальної інженерії.

Важливим аспектом є також ризики, пов'язані з технологічною залежністю органів державної влади від зовнішніх постачальників програмного забезпечення та обладнання. Це створює потенційні загрози для національної безпеки та суверенітету держави в інформаційній сфері. У цьому контексті актуальним є визначення "цифрового суверенітету" як "здатності держави самостійно і незалежно визначати свої внутрішні та геополітичні національні інтереси в цифровому середовищі" (Петров, 2021, с. 23).

Дослідження також виявило ризики, пов'язані з можливістю маніпулювання даними та інформацією в цифровому середовищі. Це може призвести до прийняття неправильних управлінських рішень та підриву довіри громадян до органів державної влади. Важливим завданням є розробка механізмів верифікації інформації та забезпечення її достовірності в процесі цифрової взаємодії.

Окремої уваги заслуговують соціально-економічні ризики діджиталізації, зокрема, можливе зростання безробіття серед державних службовців внаслідок автоматизації процесів. За прогнозами експертів, до 2030 року до 30% робочих місць у державному секторі можуть бути автоматизовані (Інститут економіки та прогнозування НАН України, 2023, с. 56). Це вимагає розробки стратегій перекваліфікації кадрів та адаптації системи державної служби до нових умов.

Важливого значення набувають ризики, пов'язані з правовим регулюванням процесів діджиталізації. Існуючі прогалини в законодавстві створюють невизначеність щодо відповідальності за кіберінциденти, захисту прав громадян у цифровому середовищі та регулювання нових форм електронної взаємодії між державою та суспільством. Це підкреслює необхідність подальшого вдосконалення нормативно-правової бази з урахуванням сучасних викликів цифрової трансформації.

Висновки.

Аналіз ризиків та загроз діджиталізації в органах державної влади дозволяє зробити ряд важливих висновків. Перш за все, необхідно підкреслити, що цифрова трансформація державного управління є невідворотним процесом, який, попри наявність певних ризиків, несе в собі значний потенціал для підвищення ефективності та прозорості діяльності органів влади. Водночас, ігнорування потенційних загроз може призвести до серйозних негативних наслідків як для держави, так і для суспільства в цілому.

Одним із ключових висновків є необхідність комплексного підходу до забезпечення інформаційної безпеки та кіберзахисту в умовах діджиталізації. Це передбачає не лише впровадження технічних засобів захисту, але й розвиток культури кібербезпеки серед державних службовців та громадян. Важливим

завданням є також створення ефективної системи реагування на кіберінциденти та розробка планів безперервності діяльності органів державної влади в умовах кіберзагроз (Бакалінська, & Бакалинський, 2019, с. 100-108).

Дослідження підтвердило критичну важливість розвитку цифрових компетенцій як серед працівників органів державної влади, так і серед населення в цілому. Підвищення рівня цифрової грамотності є ключовим фактором мінімізації ризиків, пов'язаних з людським фактором у процесі цифрової трансформації. У цьому контексті важливо розробити та впровадити комплексні програми навчання та підвищення кваліфікації, які б враховували специфіку діяльності органів державної влади (Гнатюк, 2022, с. 34).

Важливим висновком є необхідність забезпечення балансу між впровадженням інноваційних технологій та збереженням цифрового суверенітету держави. Це вимагає розробки стратегії розвитку вітчизняного IT-сектору, стимулювання створення власних програмних продуктів та технологічних рішень для потреб державного управління. Водночас, важливо забезпечити інтеграцію українських цифрових систем у глобальне інформаційне середовище з дотриманням міжнародних стандартів безпеки та захисту даних (Семенченко, Жиляєв, 2020, с. 67).

Дослідження також підкреслило необхідність вдосконалення нормативно-правової бази у сфері діджиталізації державного управління. Зокрема, актуальним є прийняття комплексного закону про цифрову трансформацію, який би визначав основні принципи, механізми та відповідальність учасників процесу цифровізації. Важливо також гармонізувати українське законодавство з міжнародними нормами у сфері кібербезпеки та захисту персональних даних.

Аналіз соціально-економічних ризиків діджиталізації вказує на необхідність розробки стратегії адаптації ринку праці до нових умов цифрової економіки. Це передбачає не лише перекваліфікацію кадрів, але й створення нових робочих місць у сфері цифрових технологій, розвиток інноваційних напрямків діяльності в державному секторі. Важливо забезпечити соціальний захист працівників, чиї посади можуть бути автоматизовані, та сприяти їх плавному переходу до нових форм зайнятості (Колот, & Герасименко, 2023, с. 123).

Дослідження підтвердило важливість забезпечення інклюзивності процесу діджиталізації. Необхідно розробити механізми, які б гарантували доступ до цифрових державних послуг для всіх категорій населення, включаючи людей з обмеженими можливостями, літніх людей та мешканців віддалених регіонів. Це вимагає не лише технологічних рішень, але й просвітницької роботи та створення системи підтримки для тих, хто відчуває труднощі у використанні цифрових інструментів (Лопушняк, & Рибчанська, 2022 с. 56).

Важливою є необхідність постійного моніторингу та оцінки ризиків діджиталізації. В умовах швидкого розвитку технологій та зміни характеру загроз, органи державної влади повинні мати гнучкі системи управління ризиками, здатні оперативно реагувати на нові виклики. Це передбачає створення спеціалізованих підрозділів з оцінки ризиків, проведення регулярних аудитів безпеки та розробку сценаріїв реагування на потенційні кризові ситуації (Грицяк, & Соловйов, 2015, с. 78).

Дослідження підкреслило роль міжнародного співробітництва у сфері подолання ризиків та загроз діджиталізації. Україна повинна активно брати участь у глобальних ініціативах з кібербезпеки, обміну досвідом та розробки спільних стандартів цифрового врядування. Це дозволить не лише підвищити рівень захисту національних інформаційних систем, але й зміцнити позиції України як надійного партнера у міжнародному цифровому просторі (Кравченко, 2023, с. 45).

Підсумовуючи, можна стверджувати, що ефективне управління ризиками та загрозами діджиталізації в органах державної влади вимагає комплексного, міждисциплінарного підходу. Це передбачає поєднання технологічних, організаційних, правових та соціально-економічних заходів, спрямованих на створення безпечного та ефективного цифрового середовища державного управління. Лише за таких умов Україна зможе повною мірою реалізувати потенціал цифрової трансформації та забезпечити сталий розвиток держави в умовах глобальної цифрової економіки.

БІБЛІОГРАФІЧНІ ПОСИЛАННЯ

Бакалінська, О. О., & Бакалинський, О. О. (2019). Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*, 9/2019, 100-108. Відновлено з http://pgp-journal.kiev.ua/archive/2019/9/18.pdf

Гнатюк, С. Л. (2022). Цифрові компетенції державних службовців: виклики та перспективи. *Стратегічні пріоритети*, 1(61), 30-38.

Грицяк, Н. В., & Соловйов, С. Г. (2015). *Електронна демократія: навч. посіб*. Київ: НАДУ. Відновлено з http://school26.edukit.mk.ua/Files/ downloads/455b986a-6273-409a-bb70-b391d5c660a3.pdf

Державна служба спеціального зв'язку та захисту інформації України. (2024). *Аналітична доповідь про стан кібербезпеки в Україні у 2023 році*. Київ,

Золотар, О. О. (2022). *Інформаційна безпека людини: теорія і практика*. (Монографія). Київ : АртЕк, Відновлено з. https://pdf.lib.vntu.edu.ua/books/2021/ Zolotar_2018_446.pdf.

Інститут економіки та прогнозування НАН України. (2023). *Вплив цифровізації на ринок праці в Україні*: прогнози та сценарії. Київ.

Карпенко, О. В. (2020). Цифрове врядування: імперативи реалізації в Україні. *Актуальні проблеми державного управління*, 1(81), 8-15. Відновлено з https://files.znu.edu.ua/files/Bibliobooks/Inshi71/0052080.pdf

Карпенко, О. В. (2021). Механізми формування та реалізації сервісно-орієнтованої державної політики в умовах цифровізації. *Актуальні проблеми державного управління*, 2(82), 20-27.

Колот, А. М., & Герасименко, О. О. (2023). Цифрова трансформація та нова економіка: імперативи розвитку. Економіка України, 9-10, 117-131.

Кравченко, С. О. (2023). Міжнародне співробітництво у сфері цифрового врядування: досвід для України. *Публічне управління та митне адміністрування*, 2(33), 41-49.

Куйбіда, В. С. (2019). Цифрове врядування в Україні: проблеми та перспективи розвитку. *Збірник наукових праць Національної академії державного управління при Президентові України*, 1, 52-61.

Куйбіда, В. С., Карпенко, О. В., & Наместнік, В. В. (2018). Цифрове врядування в Україні: базові дефініції понятійно-категоріального апарату. *Вісник Національної академії державного управління при Президентові України. Серія: Державне управління*, 1, 5-10. Відновлено з http://nbuv.gov.ua/UJRN/vnaddy_2018_1_3.

Лопушняк, Г. С., & Рибчанська, Х. В. (2022). Електронні послуги в системі публічного управління: інклюзивний підхід. *Ефективність державного управління*, 2(71), 51-63.

Міністерство цифрової трансформації України. (2023). *Цифрова грамотність населення України: аналітичний звіт*. Київ.

Міхровська, М. С. (2021). Цифрова трансформація держави: вплив на соціально-економічний розвиток України. *Економіка та держава*, 4, 85-92.

Орлов, О. В. (2019). *Інноваційні процеси в державному управлінні*. (Монографія). Харків: Вид-во ХарРІ НАДУ "Магістр".

Орлов, О. В. (2020). Правові аспекти цифровізації публічного управління в Україні. *Теорія та практика державного управління*, 2(69), 31-38.

Петров, Р. А. (2021). Цифровий суверенітет держави в умовах глобалізації. *Правова держава*, 42, 20-28.

Семенченко, А. І., & Жиляєв, І. Б. (2020). *Електронне урядування та електронна демократія: навч. посіб*. Київ: ФОП Москаленко О. М.

Степанов, В. Ю. (2020). Сучасні інформаційні загрози та методи боротьби з ними в умовах цифровізації державного управління. *Державне управління: теорія та практика*, 1, 62-71.

REFERENCES

Bakalinska, O. O., & Bakalinsky, O. (2019). AT. Legal provision of cyber security in Ukraine. *Entrepreneurship, economy and law*, № 9/2019. 100-108 p. Retrieved from http://pgp-journal.kiev.ua/archive/2019/9/18.pdf

Hnatiuk, S. L. (2022). Digital competencies of civil servants: challenges and prospects. *Strategic priorities*, 1(61), 30-38.

Hrytsyak, N. V., & Solovyov, S. G. (2015). *Electronic democracy: teaching. manual*. Kyiv: NADU, 2015. Retrieved from http://school26. edukit.mk.ua/Files/downloads/455b986a-6273-409a-bb70-b391d5c660a3.pdf

Institute of Economics and Forecasting of the National Academy of Sciences of Ukraine. (2023). *Impact of digitization on the labor market in Ukraine: forecasts and scenarios*. Kyiv.

Karpenko, O. V. (2020). Digital governance: imperatives of implementation in Ukraine. *Actual problems of public administration*, 1(81), 8-15. Retrieved from https://files.znu.edu.ua/files/Bibliobooks/Inshi71/0052080.pdf

Karpenko, O. V. (2021). Mechanisms of formation and implementation of service-oriented state policy in conditions of digitalization. *Actual problems of public administration*, 2(82), 20-27.

Kolot, A. M., & Gerasimenko, O. O. (2023). Digital transformation and the new economy: development imperatives. Economy of Ukraine, 9-10, 117-131.

Kravchenko, S. O. (2023). International cooperation in the field of digital governance: experience for Ukraine. *Public administration and customs administration*, 2(33), 41-49.

Kuybida, V. S. (2019). Digital governance in Ukraine: problems and development prospects. Collection of scientific works of the National Academy of Public Administration under the President of Ukraine, 1, 52-61.

Kuybida, V. S., Karpenko, O. V., & Namestnik, V. V. (2018). Digital governance in Ukraine: basic definitions of the conceptual and categorical apparatus. *Bulletin of the National Academy of Public Administration under the President of Ukraine. Series: Public administration*, 1, 5-10. Retrieved from http://nbuv.gov.ua/UJRN/vnaddy_2018_1_3.

Lopushnyak, G. S., & Rybchanska, H. V. (2022). Electronic services in the public administration system: an inclusive approach. *Effectiveness of public administration*, 2(71), 51-63.
Mikhrovska, M. S. (2021). Digital transformation of the state: impact on the socio-economic development of Ukraine. *Economy and the state*, 4, 85-92.
Ministry of Digital Transformation of Ukraine. (2023). *Digital literacy of the population of Ukraine: analytical report*. Kyiv.
Orlov, O. V. (2019). *Innovative processes in state administration*. (Monograph). Kharkiv: Publishing House of KhaRI NADU "Master".
Orlov, O. V. (2020). Legal aspects of digitalization of public administration in Ukraine. *Theory and practice of public administration*, 2(69), 31-38.
Petrov, R. A. (2021). Digital sovereignty of the state in the conditions of globalization. *Rule of law*. No. 42. P. 20-28.
Semenchenko, A. I., & Zhilyaev, I. B. (2020). *Electronic governance and electronic democracy: teaching. manual*. Kyiv: FOP Moskalenko O. M..
State Service of Special Communications and Information Protection of Ukraine. (2024). *Analytical report on the state of cyber security in Ukraine in 2023*. Kyiv.
Stepanov, V. Yu. (2020). Modern informational threats and methods of combating them in the conditions of digitalization of public administration. *Public administration: theory and practice*, 1, 62-71.
Zolotar, O. O. (2022). Human information security: theory and practice. (Monograph). Kyiv: ArtEk. Retrieved from https://pdf.lib.vntu.edu.ua/books/2021/ Zolotar_2018_446.pdf.