УДК 351
https://doi.org/10.32689/2617-2224-2024-2(39)-9

Чуба Назар Володимирович,
аспірант кафедри публічного адміністрування, ПрАТ «ВНЗ «Міжрегіональної Академії управління персоналом», 03039, м. Київ вул. Фрометівська, 2, e-mail: nazarmsx@ukr.net, https://orcid.org/0000-0002-7727-3627

Chuba Nazar Volodymyrovych,
Postgraduate Student at the Department of Public Administration, Interregional Academy of Personnel Management, 03039, Kyiv, Frometivska str., 2, e-mail: nazarmsx@ukr.net, https://orcid.org/0000-0002-7727-3627

РОЗБУДОВА ЕЛЕКТРОННОГО УРЯДУВАННЯ: ЗАГРОЗИ ТА ВИКЛИКИ

Анотація. Метою роботи є визначення основних загроз та викликів, з якими стикаються ініціативи електронного урядування в сучасному контексті та формулювання пропозицій щодо пом'якшення наслідків виявлених загроз і викликів.

Методологія. Розглянуто теоретичні підходи у працях науковців щодо виявлення сучасних викликів та загроз у системі електронного урядування, застосовано сучасні методологічні підходи до визначення рівня розвитку електронного врядування та кіберзагроз на основі світових рейтингів (Індекс розвитку електронного урядування, Національний індекс кібербезпеки). В аналізі показників використано графічні методи порівняння.

Наукова новизна. Встановлено ключову проблематику, що пов'язана з розвитком електронного урядування (гарантування кібербезпеки, захист конфіденційності, опір змінам, організаційна динаміка, корупційні зловживання). Визначено основні шляхи подолання перешкод на шляху упровадження електронного урядування в Україні: регулярний технологічний аудит, постійний моніторинг технологічних тенденцій, створення інноваційних хабів, розвиток технологічних навичок, управління змінами та подолання опору, комунікації та розвиток лідерства.

Висновки. Електронне урядування потребує адаптивності та стратегічного прогнозування через динамічний характер вказаної сфери. За умови ефективного впровадження, воно здатне зробити систему державного управління прозорішою та орієнтованою на громадян. Водночас існують виклики – ризики кібербезпеки, проблеми конфіденційності даних, опір змінам. Очікувані тенденції технологічного розвитку (блокчейн, штучний інтелект) визначатимуть майбутнє електронного урядування, створюючи нові можливості та очікуючи появу загроз. Тому держава має передбачати майбутні тренди та використовувати інновації для побудови стійких систем електронного урядування, долаючи окремі труднощі розвитку.

Ключові слова: електронне урядування, виклики, кіберзагрози, державне управління, політика, надання послуг, цифровізація, діджиталізація.

THREATS AND CHALLENGES RELATED TO ELECTRONIC GOVERNMENT

Abstract. The purpose of the work is to identify the main threats and challenges faced by e-government initiatives in the modern context and to formulate proposals for mitigating the consequences of the identified threats and challenges.

Methodology. The theoretical approaches in the works of scientists regarding the identification of modern challenges and threats in the e-government system were considered, and modern methodological approaches were applied to determine the level of development of e-government and cyber threats based on world ratings (e-Government Development Index, National Cyber Security Index). Graphical methods of comparison are used in the analysis of indicators.

Scientific novelty. Key issues related to the development of e-government (guaranteeing cyber security, privacy protection, resistance to change, organizational dynamics, corruption abuses) have been identified. The main ways to overcome obstacles to the implementation of e-government in Ukraine are identified: regular technological audit, constant monitoring of technological trends, creation of innovation hubs, development of technological skills, change management and overcoming resistance, communication and leadership development.

Conclusions. Electronic governance requires adaptability and strategic forecasting due to the dynamic nature of the specified area. Provided it is effectively implemented, it can make the public administration system more transparent and citizen-oriented. At the same time, there are challenges – cyber security risks, data privacy issues, resistance to change. Expected technological development trends (blockchain, artificial intelligence) will determine the future of e-government, creating new opportunities and anticipating threats. Therefore, the state must anticipate future trends and use innovations to build sustainable e-government systems, overcoming certain development difficulties.

Key words: e-government, challenges, cyber threats, public administration, politics, service provision, digitization, digitalization.

Постановка проблеми. Електронне урядування спричинило суттєві трансформації в системі державного управління в усьому світі. Розвиток інформаційно-комунікаційних технологій дозволив органам державної влади впроваджувати цифрові рішення, переосмислюючи способи взаємодії громадян з державою та змінюючи усталені адміністративні процеси. В останні декілька десятиліть впровадження ініціатив з електронного урядування стало однією з ключових реформ більшості розвинених країн. Органи влади дедалі активніше використовують цифрові технології для оптимізації роботи, покращення надання послуг та сприяння залученню громадян. Перехід до цифрового врядування виявив себе підвищенням ефективності, прозорості та доступності державних послуг. Широке розповсюдження смартфонів, підключення до Інтернету та цифрових платформ прискорило зазначену глобальну тенденцію, зробивши електронне урядування головним рушієм адміністративних інновацій.

Підходи електронного урядування переосмислили традиційні бюрократичні моделі з акцентом на використанні технологій для створення гнучких, орієнтованих на громадян і керованих даними управлінських структур. Електронне урядування виходить за межі лише оцифрування існуючих процесів, знаменуючи зміну парадигми у бік відкритого, ефективного та підзвітного врядування. Оскільки держава стикається зі складними викликами, починаючи від урбанізації і закінчуючи глобальними кризами, електронне урядування виявляє себе в якості інструменту для підвищення стійкості та оперативності системи державного управління. В той же час, вкрай важливо визначити сучасну проблематику подальшого впровадження електронного урядування та основні виклики, які постають на цьому шляху.

Аналіз останніх досліджень і публікацій. Питання, пов'язані із розвитком електронного урядування розглядали у власних працях зарубіжні та вітчизняні науковці: А. Ільїна, М. Кота, А. Лісняк, І. Погребняк, Ф. Са, В. Фалькевич, Б. Франк та багато інших. Не применшуючи існуючі наукові дослідження, слід відзначити потребу зосередитися на наявних викликах та загрозах, які виникають у процесі реалізації електронного врядування.

Мета дослідження – визначити основні загрози та виклики, з якими стикаються ініціативи електронного урядування в сучасному контексті та формулювання пропозицій щодо пом'якшення наслідків виявлених загроз і викликів.

Виклад основного матеріалу дослідження. Електронне урядування розглядається як багатокритеріальні процеси використання

інформаційно-комунікаційних технологій для надання державних послуг та покращення роботи органів державної влади (Sá et al., 2016). І. Погребняк розглядає електронне врядування як клієнторієнтовану систему, спрямовану на задоволення різних вимог та очікувань споживачів державних послуг (Погребняк, 2014). Цифровізація адміністративних процесів та інтерфейсів має на меті підвищити ефективність, прозорість, зручність та розширену участь громадськості. Однак на практиці ініціативи електронного урядування стикаються з різними загрозами та ризиками, починаючи від кібератак і закінчуючи опором змінам.

Основна загроза пов'язана з уразливістю безпеки даних, через яку персональні дані громадян та конфіденційна інформація органів влади піддаються несанкціонованому доступу або крадіжці. Електронне урядування централізує оцифровані бази даних у взаємопов'язаних системах, що збільшує ризики, незважаючи на існуючі засоби контролю доступу. Опитані фахівці з урядових технологій відзначили внутрішні загрози від корумпованих державних службовців, які зловживають привілеями доступу (Falkevych & Lisnyak, 2023). Зовнішні кібератаки також компрометують зміст державних документів, причому зростає тенденція до атак з використанням програм-вимагачів, які шифрують державні дані, використовуючи вразливості в програмному забезпеченні, що не були виправлені.

Об'єднуючи різні бази даних громадян, електронне урядування також підвищує ризики порушення приватності через програми масового спостереження, які відстежують діяльність без належного нагляду (Antoine, 2022; Rouibah et al., 2022). Після поєднання персональні дані можуть бути використані для незаконного стеження за допомогою сучасних технологій, які порушують основні права.

Експерти наголошують на навчанні з кібербезпеки, а також на надійних засобах управління ідентифікацією та доступом для пом'якшення внутрішніх загроз, підкріплених шифруванням, виявленням аномалій, брандмауерами і тестуванням вразливостей (Jiang et al., 2022). Резервування за допомогою копіювання даних, альтернативних сайтів і протоколів відновлення після аварій також сприяє підвищенню стійкості. Однак контроль над технологіями вимагає відповідної політики підзвітності, включаючи обов'язкове звітування про кіберінциденти, щоб забезпечити швидке усунення порушень у разі їх виникнення (Franck & Reith, 2022).

Електронне урядування, хоч і є трансформаційним, але породжує безліч ризиків кібербезпеки, які становлять значну загрозу для державних ініціатив. Однією з головних проблем є потенційна можливість кібератак, які можуть порушити основні функції органів державної влади та скомпрометувати конфіденційну інформацію. Кіберзагрози охоплюють цілий спектр зловмисних дій, включаючи хакерство, програми-вимагачі та розподілені атаки.

Аналіз вразливостей цифрових систем має вирішальне значення для розуміння потенційних кіберзагроз. Вплив кібератак виходить за рамки операційних збоїв і охоплює оприлюднення даних громадян, підрив суспільної довіри та потенційні економічні наслідки. З метою зменшення ризиків кібербезпеки, держава повинна прийняти комплексні стратегії, які включають надійні протоколи кібербезпеки, регулярний аудит систем і постійне навчання співробітників.

Україна робить суттєві кроки щодо посилення систем захисту державних електронних ресурсів та платформ. Порівняння національного індексу кібербезпеки України з деякими європейськими країнами (рис. 1) свідчить про досягнення достатньо високого рівня у зазначеній сфері.

Таким чином, кіберризики, питання конфіденційності, бар'єри для впровадження та корупційні зловживання є ключовими загрозами, які можуть суттєво погіршити результати електронного урядування. Багатогранний підхід, що поєднує технологічні гарантії, політику нагляду, розвиток потенціалу та розбудову суспільної довіри, має важливе значення для максимізації можливостей покращення послуг, прозорості та впливу на державну політику через цифрову трансформацію органів влади.

Цифровий розрив створює бар'єри для впровадження електронного урядування серед окремих громад з низьким рівнем доступу до інформаційно-комунікативних технологій або цифрової грамотності (Masadeh et al., 2023). Комплексне управління змінами є іншим напрямом проблематики, оскільки державні службовці чинять опір новим вимогам прозорості, а громадяни не довіряють доступу до Інтернету, який замінює традиційні канали (Wang et al., 2023). Значна кількість програм електронного урядування, що реалізуються під керівництвом держави, не використовуються повною мірою через низький рівень впровадження. Недостатнє фінансування також перешкоджає використанню складних систем, які залежать від розвиненої інфраструктури та кваліфікованого персоналу, якого бракує багатьом органам влади (Ільїна, 2020).

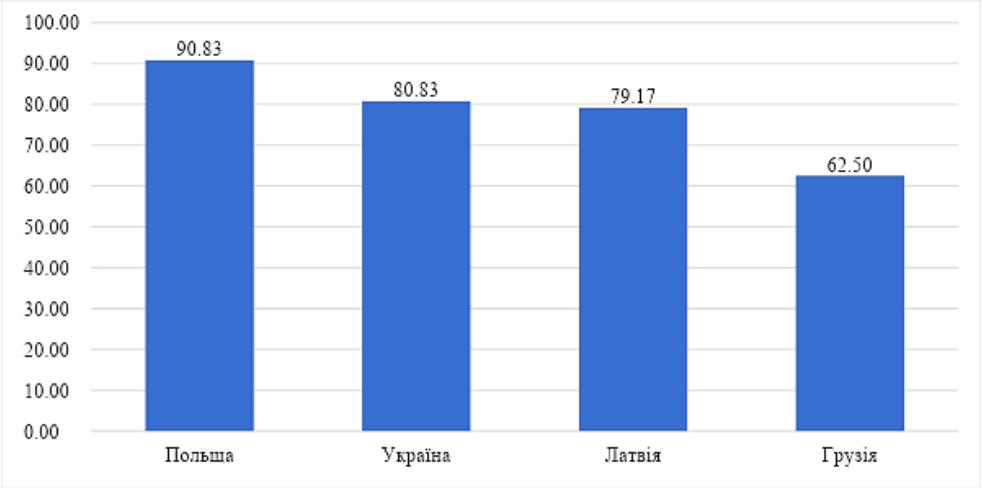

Рис. 1. Національний індекс кібербезпеки окремих країн, 2024 р. (NCSI, 2024)

В останні десятиліття еволюція електронного урядування характеризується інтеграцією нових технологій. Мобільні додатки, аналітика даних і штучний інтелект сьогодні відіграють важливу роль в оптимізації адміністративних процесів і створенні персоналізованого досвіду для громадян. Відслідковуючи прогрес у сфері реалізації електронного урядування, необхідно орієнтуватися на певні незалежні оцінки для подальшого удосконалення окремих напрямів.

Індекс розвитку електронного урядування (EGDI) відображає орієнтовані на громадян ініціативи в галузі електронного урядування. Аналіз показників розвитку електронного урядування (EGDI) України у порівнянні зі світовим лідером та субрегіональним лідером (рис. 2) демонструє певне відставання, яке поступово долається. В цілому Україна займає 46 місце зі 193 країн (UN, 2022), що свідчить про значний прогрес, здійснений державою.

Розглянемо детально компоненти Індексу розвитку електронного урядування України (рис. 3). Виходячи з наявних даних, держава має здійснити необхідні зусилля щодо модернізації наявної телекомунікаційної інфраструктури, що потребує значних інвестиційних ресурсів.

Зазначене підкреслює важливість стратегічного планування, орієнтованого на користувача державних електронних платформ та надійної технологічної інфраструктури. Безпека даних, співпраця зацікавлених сторін і прагнення до постійного вдосконалення є чинниками успішної реалізації ініціатив у сфері електронного урядування.

Оскільки електронне урядування значною мірою спирається на збір та обробку даних громадян, питання конфіденційності даних постає дуже гостро. Несанкціонований доступ, витоки даних і неналежне поводження з інформацією можуть поставити під загрозу приватність гро-

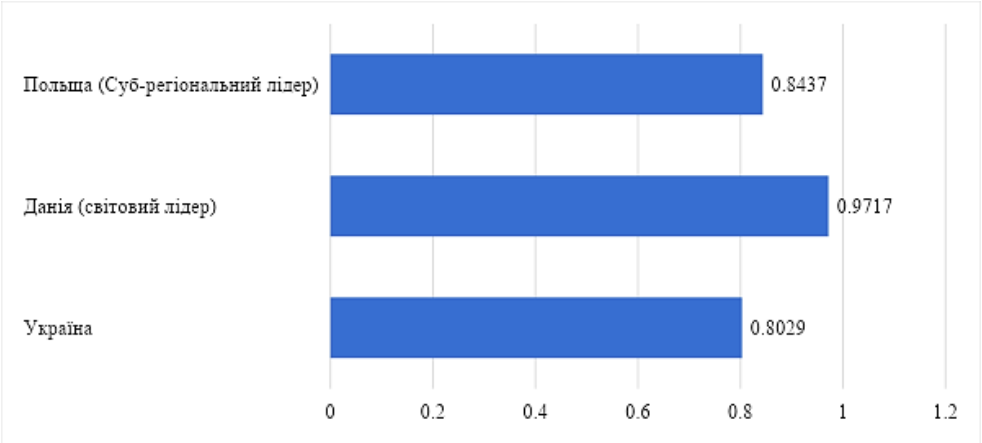

Рис. 2. Порівняння індексу розвитку електронного урядування, 2022 р. (UN, 2022)

Рис. 3. Компоненти EGDI України, 2023 р. (UN, 2023)

мадян і підірвати довіру до цифрових ініціатив держави. Наслідки витоку даних виходять за межі безпосередньої шкоди і можуть призвести до крадіжки персональних даних, фінансових втрат або навіть маніпулювання демократичними процесами.

Хоча електронне урядування обіцяє розширити доступ до державних послуг, існує ризик поглиблення існуючої цифрової нерівності. Цифрова нерівність проявляється в різних формах, включаючи нерівність у доступі до Інтернету, цифровій грамотності та впровадженні технологій. Вразливі верстви населення, наприклад, мешканці сільської місцевості, можуть стикатися з перешкодами у доступі до послуг електронного урядування та користуванні ними. Вирішення нагальних проблем вимагає багатогранного підходу, який враховує розвиток інфраструктури, програми цифрової освіти та цільові ініціативи з подолання цифрового розриву.

Держава має визначити пріоритетами вдосконалення цифрової інфраструктури, підвищення цифрової грамотності за допомогою освітніх програм і забезпечення розробки послуг електронного урядування з урахуванням різноманітних потреб користувачів. Крім того, постійні оцінки впливу ініціатив електронного урядування на різні демографічні групи є важливими для виявлення та усунення нерівностей, що виникають.

Однією з основних проблем, що виникають при впровадженні електронного урядування, є опір, з яким стикаються органи влади та адміністративні структури. Перехід від традиційних адміністративних процесів до цифрових систем часто зустрічає скептицизм і небажання серед державних службовців, які звикли до усталених робочих процесів і можуть чинити опір впровадженню електронного урядування через побоювання щодо збереження робочих місць, зміни ролей і незнання технологій.

Стратегії подолання організаційної інерції передбачають комплексний підхід, який включає практики управління змінами, комунікаційні стратегії та програми розвитку навичок. Залучення зацікавлених сторін до процесу переходу, розвиток культури інновацій і забезпечення належного навчання можуть допомогти зменшити побоювання і сприяти більш плавній інтеграції електронного урядування в бюрократичні структури.

Електронне урядування функціонує в складному нормативно-правовому середовищі, яке може створювати значні труднощі на шляху його впровадження. Найбільше занепокоєння викликають проблеми, пов'язані з дотриманням законодавства про захист даних і приватності. Органи державної влади повинні дотримуватися балансу між використанням даних громадян для покращення якості послуг і захистом прав громадян на недоторканність приватного життя.

Аналіз ризику технологічного старіння передбачає проактивну оцінку терміну придатності впроваджених систем і виявлення нових технологій, які можуть замінити або вдосконалити існуючі рішення. Щоб протистояти наявному виклику, держава повинна прийняти масштабований підхід до впровадження технологій, що дозволить інтегрувати нові технології без капітального ремонту всієї системи, забезпечуючи стійкість і адаптивність. Підходи до забезпечення сталості систем електронного урядування включають регулярний технологічний аудит, постійний моніторинг технологічних тенденцій та створення інноваційних хабів.

Упровадження принципів забезпечення конфіденційності при розробці систем електронного урядування є необхідною умовою для збереження довіри громадян та дотримання законодавства про захист персональних даних. Рекомендація цих принципів передбачає врахування міркувань конфіденційності на кожному етапі проєктування та експлуатації електронних систем.

Отже, впровадження електронного урядування є не лише технологічним процесом, а цілісною трансформацією, яка вимагає поєднання розгляду питань кібербезпеки, конфіденційності та організаційної динаміки. Комплексні програми розбудови спроможності повинні охоплювати технологічні навички, управління змінами, комунікації та розвиток лідерства. Визнання різноманітних потреб державних службовців має вирішальне значення для розробки програм, спрямованих на подолання конкретних бар'єрів, що перешкоджають впровадженню електронного урядування.

Висновки. Електронне урядування є сферою, яка постійно розвивається та вимагає адаптивності та стратегічного прогнозування. Необхідність заходів для подолання загроз і викликів підкреслює потребу в постійному удосконаленні та інноваціях у сфері електронного урядування.

За умови ефективного впровадження, електронне урядування здатне кардинально змінити систему державного управління, зробивши її більш прозорою, доступною та орієнтованою на громадян. Однак на цьому трансформаційному шляху є чимало викликів, зокрема ризики кібербезпеки, проблематика дотримання конфіденційності даних, опір змінам та ін. Очікувані тенденції в електронному урядуванні демонструють динамічний характер вказаної сфери. Блокчейн, штучний інтелект, розширена аналітика даних та інновації в галузі кібербезпеки визначатимуть майбутнє цифрового врядування. Хоча зазначені технології пропонують безпрецедентні можливості, вони також створюють нові виклики, які вимагають дієвого та адаптивного управління.

Виходячи з наявної проблематики, слід зазначити, що держава має не лише вирішувати поточні проблеми, але й передбачати та використовувати нові тенденції для побудови стійких, орієнтованих на громадян систем електронного урядування. Реалізація ефективної системи електронного урядування має поряд з окремими викликами і значні успіхи, що виникають на шляху постійного прагнення до інновацій, адаптивності та дотримання принципів прозорості у наданні ключових державних послуг.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Ільїна А. О. Проблеми розвитку електронного урядування в органах публічної влади України та шляхи їх вирішення. *Експерт: парадигми юридичних наук і державного управління*. 2020. №. 2 (8). С. 232–249. DOI: https://doi.org/10.32689/2617-9660-2020-2(8)-232-249.
2. Погребняк І. Є. Електронний уряд (e-government) і електронне урядування (e-governance): поняття та принципи функціонування. *Право та інновації*. 2014. №. 3. С. 26–35.
3. Antoine L. The power of a promise: whom do governments' security justifications convince to accept surveillance?. *Political Research Exchange*. 2022). № 4. DOI: https://doi.org/10.1080/2474736X.2022.2101380.
4. Falkevych V., Lisnyak A. Internal and External Threats in Cyber Security and Methods for Their Prevention. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE, 2023. P. 414–419. DOI: 10.1109/ACIT58437.2023.10275516.
5. Franck B., Reith M. Operationalizing Cyber: Recommendations for Future Research. *European Conference on Cyber Warfare and Security*. 2022. DOI: https://doi.org/10.34190/eccws.21.1.308.
6. Jiang Y., et al. Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2022. №52(12). P. 7799–7809. DOI: https://doi.org/10.1109/TSMC.2022.3164024
7. Masadeh R., Almajal D., Majali T., Majali S., Al-Sherideh A. An empirical study into the effect of the digital divide on the intention to adopt e-government. *International Journal of Data and Network Science*. 2023. № 7. DOI: https://doi.org/10.5267/j.ijdns.2023.8.005.
8. National Cyber Security Index. *NCSI*, 2024. URL: https://ncsi.ega.ee/.
9. Rouibah K., Qurban H., Al-Qirim N. Impact of Risk Perceptions and User Trust on Intention to Re-Use E-Government: A Mixed Method Research. *J. Glob. Inf. Manag.* 2022. №30. P. 1–29. DOI: https://doi.org/10.4018/jgim.307117.
10. Sa F., Rocha A., Cota M. P. Potential dimensions for a local e-Government services quality model. *Telematics and Informatics*. 2016. №33(2). P. 270–276. DOI: https://doi.org/10.1016/j.tele.2015.08.005.
11. Semenets-Orlova I., Rodchenko L., Chernenko I., Druz O., Rudenko M., & Poliuliakii R. Requests for public information in the state Administration in situations of military operations. *Ann. Fac. Der. U. Extremadura*, 2022, *38*, 249.
12. Semenets-Orlova I. A. Derzhavne upravlinnia osvitnimy zminamy v Ukraini: teoretychni zasady [Public Management of Educational Change in Ukraine: Theoretical Principles]. *Kyiv: YuSPTON [in Ukrainian]*, 2018.
13. Semenets-Orlova I. Procedural aspects of educational changes: empirical findings at institutional level. *Advanced Education*, 2017, 7, 64–67.
14. United Nations e-government survey. 2022. UN, 2022. URL: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf.
15. United Nations e-government survey. 2023. UN, 2023. URL: https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf.
16. Wang Z., Liu H., Li T., Zhou L., Zhou M. The Impact of Internet Use on Citizens' Trust in Government: The Mediating Role of Sense of Security. *Systems*. 2023. № 11 P. 47. DOI: https://doi.org/10.3390/systems11010047.

REFERENCES:

1. Ilyina, A. O. (2020). Problemy rozvytku elektronnoho uryaduvannya v orhanakh publichnoyi vlady Ukrayiny ta shlyakhy yikh vyrishennya [Problems of the development of electronic governance in public authorities of Ukraine and

ways of their solution]. *Expert: Paradigm of Law and Public Administration*, 2(8), 232–249. https://doi.org/10.32689/2617-9660-2020-2(8)-232-249 [in Ukrainian].
2. Pogrebnyak, I. E. (2014). Elektronnyy uryad (e-government) i elektronne uryaduvannya (e-governance): ponyattya ta pryntsypy funktsionuvannya [Electronic government (e-government and e-governance (e-governance): concept and principles of operation]. *Law and innovation*, №. 3, 26–35 [in Ukrainian].
3. Antoine, L. The power of a promise: whom do governments' security justifications convince to accept surveillance?. *Political Research Exchange*. 2022). № 4. DOI: https://doi.org/10.1080/24747 36X.2022.2101380.
4. Falkevych, V., Lisnyak, A. (2023). Internal and External Threats in Cyber Security and Methods for Their Prevention. *2023 13th International Conference on Advanced Computer Information Technologies (ACIT)*. IEEE, P. 414–419. DOI: 10.1109/ ACIT58437.2023.10275516.
5. Franck, B., Reith, M. (2022). Operationalizing Cyber: Recommendations for Future Research. *European Conference on Cyber Warfare and Security*. DOI: https://doi.org/10.34190/eccws.21.1.308.
6. Jiang, Y., et al. (2022). Secure data transmission and trustworthiness judgement approaches against cyber-physical attacks in an integrated data-driven framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. №52(12). P. 7799–7809. DOI: https://doi.org/10.1109/TSMC.2022.3164024 .
7. Masadeh, R., Almajal, D., Majali, T., Majali, S., Al-Sherideh, A. (2023). An empirical study into the effect of the digital divide on the intention to adopt e-government. *International Journal of Data and Network Science*. № 7. DOI: https://doi.org/10.5267/ j.ijdns.2023.8.005.
8. National Cyber Security Index. *NCSI*, 2024. Retrieved from: https://ncsi.ega.ee/.
9. Rouibah, K., Qurban, H., Al-Qirim, N. (2022). Impact of Risk Perceptions and User Trust on Intention to Re-Use E-Government: A Mixed Method Research. *J. Glob. Inf. Manag.* №30. P. 1–29. DOI: https://doi.org/10.4018/jgim.307117.
10. Sa, F., Rocha, A., Cota ,M. P. (2016). Potential dimensions for a local e-Government services quality model. *Telematics and Informatics*. №33(2). P. 270–276. DOI: https://doi.org/10.1016/j.tele.2015.08.005.
11. Semenets-Orlova, I., Rodchenko, L., Chernenko, I., Druz, O., Rudenko, M., & Poliuliakii, R. (2022). Requests for public information in the state Administration in situations of military operations. *Ann. Fac. Der. U. Extremadura*, *38*, 249.
12. Semenets-Orlova, I. A. (2018). Derzhavne upravlinnia osvitnimy zminamy v Ukraini: teoretychni zasady [Public Management of Educational Change in Ukraine: Theoretical Principles]. Kyiv: YuSPTON [in Ukrainian].
13. Semenets-Orlova, I. (2017). Procedural aspects of educational changes: empirical findings at institutional level. *Advanced Education*, 7, 64–67.
14. United Nations e-government survey. 2022. UN, 2022. Retrieved from: https://desapublications. un.org/sites/default/files/publications/2022-09/ Web%20version%20E-Government%202022.pdf.
15. United Nations e-government survey. 2023. UN, 2023. Retrieved from: https://desapublications. un.org/sites/default/files/publications/2022-09/ Web%20version%20E-Government%202022.pdf.
16. Wang, Z., Liu, H., Li, T., Zhou, L., Zhou, M. (2023). The Impact of Internet Use on Citizens' Trust in Government: The Mediating Role of Sense of Security. *Systems*. № 11 P. 47. DOI: https://doi.org/10.3390/ systems11010047.