ISSN (print) 2708-7530
Наукові перспективи № 4(46) 2024

УДК 004.056.5:351.78

https://doi.org/10.52058/2708-7530-2024-4(46)-361-370

П’ятничук Ірина Дмитрівна кандидат економічних наук, доцент, завідувачка кафедри управління та бізнес-адміністрування, Прикарпатський національний університет імені Василя Стефаника, м. Івано-Франківськ, вул. Шевченка, 57, https://orchid.org/0000-0003-2876-6422

НОРМАТИВНО-ПРАВОВИЙ МЕХАНІЗМИ ПУБЛІЧНОГО УПРАВЛІННЯ ПРОЦЕСАМИ ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ

Анотація. У сучасному цифровому світі зростає значення електронних послуг та державного управління, але разом з цим збільшується загроза для інформаційної безпеки. Нормативно-правові механізми управління процесами захисту інформаційної безпеки у сфері надання електронних послуг стають ключовими для забезпечення цифрової безпеки та довіри громадян до державних систем. Процес надання електронних послуг нерозривно пов'язаний із захистом конфіденційної інформації громадян та ефективним управлінням цими процесами. Однак існують виклики щодо розробки та вдосконалення нормативно-правових механізмів, які відповідали б вимогам сучасного цифрового середовища та забезпечували ефективний захист інформації. Метою дослідження є аналіз сучасного стану та перспектив розвитку нормативно-правових механізмів управління процесами захисту інформаційної безпеки у сфері надання електронних послуг. Об'єктом дослідження є нормативно-правові механізми управління процесами захисту інформаційної безпеки. Предметом дослідження є процес надання електронних послуг у контексті їхньої інформаційної безпеки. У дослідженні використовувалися методи аналізу та порівняльного огляду наукової літератури, а також системний аналіз нормативно-правових актів у галузі інформаційної безпеки. Проводився огляд законодавства різних країн з метою виявлення найкращих практик управління інформаційною безпекою. Автором було проведено детальний аналіз сучасного стану нормативно-правових механізмів управління процесами захисту інформаційної безпеки в контексті надання електронних послуг. Було ідентифіковано ключові проблеми та визначені напрямки для подальшого вдосконалення законодавства та практики управління інформаційною безпекою. На основі проведеного аналізу автор надає рекомендації щодо практичного впровадження результатів дослідження. Серед таких рекомендацій можуть бути вдосконалення законо-

давства, впровадження нових технологій у сферу захисту інформації та посилення міжнародного співробітництва у боротьбі з кіберзагрозами.

Ключові слова: нормативно-правові механізми, публічне управління, захист інформаційної безпеки, електронні послуги, цифрові технології, інформаційна безпека, механізми публічного управління, інформація публічні послуги

Piatnychuk Iryna Dmytrivna Candidate of Economic Sciences, associate, professor, the head of the department, Department of Management and Business, Administration, Vasyl Stefanyk Precarpathian National University, Shevchenko St., 57, Ivano-Frankivsk, https://orchid.org/0000-0003-2876-6422

REGULATORY AND LEGAL MECHANISMS OF PUBLIC MANAGEMENT OF INFORMATION SECURITY PROTECTION PROCESSES IN THE PROVISION OF ELECTRONIC SERVICES

Abstract. In today's digital world, the importance of e-services and public administration is increasing, but along with this, the threat to information security is increasing. Regulatory and legal mechanisms for managing information security protection processes in the field of providing electronic services are becoming key to ensuring digital security and citizens' trust in state systems. The process of providing electronic services is inextricably linked to the protection of confidential information of citizens and effective management of these processes. However, there are challenges regarding the development and improvement of regulatory and legal mechanisms that would meet the requirements of the modern digital environment and ensure effective information protection. The purpose of the study is to analyze the current state and prospects for the development of regulatory and legal mechanisms for managing information security protection processes in the field of providing electronic services. The object of the research is the normative and legal mechanisms of managing information security protection processes. The subject of the study is the process of providing electronic services in the context of their information security. The research used the methods of analysis and comparative review of scientific literature, as well as a systematic analysis of normative legal acts in the field of information security. A review of the legislation of various countries was conducted in order to identify the best practices of information security management. The author conducted a detailed analysis of the current state of regulatory mechanisms for managing information security protection processes in the context of providing electronic services. Key issues were identified and directions for further improvement of information security management legislation and practice were determined. Based on the analysis, the author provides

recommendations for the practical implementation of the research results. Among such recommendations may be the improvement of legislation, the introduction of new technologies in the field of information protection, and the strengthening of international cooperation in the fight against cyber threats.

Keywords: regulatory mechanisms, public administration, protection of information security, electronic services, digital technologies, information security, mechanisms of public administration, information public services

Постановка проблеми. У сучасному цифровому суспільстві, де електронні послуги стають необхідністю, питання забезпечення інформаційної безпеки відіграє критичну роль у забезпеченні довіри громадян до державних систем. Нормативно-правові механізми публічного управління процесами захисту інформаційної безпеки у сфері надання електронних послуг стають предметом серйозної уваги через постійне зростання кількості кіберзагроз та інцидентів, пов'язаних із порушенням конфіденційності та цілісності даних. Існує ризик, що із зростанням обсягів електронних послуг і цифрових технологій зростатимуть і кіберзагрози. Забезпечення ефективних нормативно-правових механізмів управління інформаційною безпекою вимагає ретельного аналізу сучасних трендів та тенденцій, а також розробки стратегічних підходів до запобігання кіберзагрозам і реагування на них. За останні роки стає очевидним зростання обсягів надання електронних послуг, що призводить до посилення уваги до нормативно-правових аспектів захисту інформації та сучасні нормативно-правові механізми управління інформаційною безпекою можуть бути недостатньо ефективними для забезпечення захисту в умовах швидко змінюючогося цифрового середовища. Відсутність міжнародної координації у сфері нормативно-правового забезпечення інформаційної безпеки може ускладнити боротьбу з кіберзагрозами. Згідно з дослідженням Європейського центру кіберзлочинності (EC3), кількість кіберзлочинів у світі зросла на 20% за останній рік. За даними Міжнародного банку реконструкції та розвитку, близько 80% країн не мають належного законодавчого забезпечення щодо кібербезпеки. З урахуванням вищезазначених викликів та тенденцій дослідження спрямоване на вивчення нових стратегій та ризиків нормативно-правової системи механізмів публічного управління процесами захисту інформаційної безпеки у сфері надання електронних послуг.

Аналіз останніх досліджень і публікацій. Актуальність теми дослідження визначається увагою авторів до розробки проблематики, зокрема, Дикий, А. П., Дика, О. С., Наумчук, К. М., Тростенюк, Т. М., Rajvanshi, P.R., Singh, T., Gupta, D. and Gupta, M., Khan, F. and Mer, A., Rangu, C.M., Badea, L., Scheau, M.C., Găbudeanu, L., Panait, I. and Radu, V., Saritepeci, M., Yildiz Durak, H., Özüdoğru, G. and Atman Uslu, N., Spagnolo, M., Ndou, V., Giribaldi, D. and Arena, V., Amonoo Nkrumah, B., Qian, W., Kaur, A. and Tilt, C., Göksan, G., Lyon, G., Nawafleh, S. and Khasawneh, A., Špaček, D. and Špačková, Z. [1-11] та інші автори.

Мета та завдання статті. Метою статті є аналіз сучасного стану та перспектив розвитку нормативно-правових механізмів управління процесами захисту інформаційної безпеки у сфері надання електронних послуг. Основний акцент робиться на ідентифікації ключових проблем, виявленні тенденцій та розробці рекомендацій щодо вдосконалення правового забезпечення в цій сфері.

Завдання дослідження:

1. Провести аналіз сучасного стану нормативно-правових механізмів публічного управління захистом інформаційної безпеки у сфері надання електронних послуг.
2. Визначити ключові проблеми та виклики, що стоять перед нормативно-правовими механізмами публічного управління інформаційною безпекою.
3. Проаналізувати сучасні тренди та тенденції у цифровому середовищі та їх вплив на ефективність захисту інформації.
4. Виявити можливості для вдосконалення законодавства та регуляторних механізмів з метою підвищення рівня інформаційної безпеки у сфері надання електронних послуг.
5. Розробити рекомендації для подальшого вдосконалення нормативно-правових механізмів управління інформаційною безпекою з урахуванням сучасних викликів та тенденцій.

Виклад основного матеріалу. У сучасному цифровому ландшафті, де використання електронних послуг стає все більшою реальністю, належне забезпечення інформаційної безпеки стає однією з ключових вимог до ефективного функціонування державних та комерційних систем. Публічне управління цими процесами вимагає належного нормативно-правового базису, спрямованого на запобігання кіберзагрозам та забезпечення конфіденційності, цілісності та доступності інформації. Аналіз сучасного стану нормативно-правових механізмів в цій області виявляє різноманітність підходів та рівень їх ефективності, який часто залежить від конкретних регуляторних рамок, які існують в кожній країні. Наприклад, деякі країни можуть мати вже встановлені закони, спрямовані на захист інформації в цифровому просторі, тоді як інші можуть знаходитися на етапі активного формування свого законодавчого середовища. Проте, незважаючи на різноманітність підходів, спільною проблемою є потреба у постійному адаптуванні нормативно-правових механізмів до швидко змінюючихся умов цифрової екосистеми. Також важливо враховувати міжнародні стандарти та норми, оскільки багато кіберзагроз та викликів виникають на міжнародному рівні і потребують спільних зусиль для ефективного контролю та протидії [1].

Таким чином, проведення аналізу сучасного стану нормативно-правових механізмів публічного управління захистом інформаційної безпеки у сфері

надання електронних послуг допоможе виявити ключові проблеми та визначити шляхи подальшого вдосконалення законодавства в цій сфері – табл. 1.

Таблиця 1

Основні проблеми публічного управління захистом інформаційної безпеки, їх негативні наслідки та способи вирішення шляхом нормативно-правових механізмів публічного управління

Основні проблеми	Негативні наслідки	Способи вирішення
Недостатня координація між різними органами та відсутність єдиного підходу до захисту інформації [2]	Підвищений ризик вразливості перед кіберзагрозами, можливість конфліктів інтересів	Створення централізованої системи управління кібербезпекою, введення чітких ролей та відповідальності
Відсутність достатньої правової бази та відповідних нормативних актів для регулювання кібербезпеки [3]	Недостатня захищеність особистих даних, ризик для національної безпеки	Розробка та прийняття нових законодавчих актів, що відповідають сучасним кіберзагрозам
Брак спеціалізованих кадрів та відповідних ресурсів для ефективного управління інформаційних злочинів [4]	Обмежений потенціал для виявлення та реагування питань з безпеки в інформативному просторі	Збільшення інвестицій у навчання та підготовку кадрів, створення спеціалізованих підрозділів
Відсутність механізмів аудиту та контролю за дотриманням встановлених правил та стандартів [5]	Збільшений ризик виникнення інцидентів безпеки та порушення конфіденційності	Впровадження систем аудиту та моніторингу з доповідністю перед відповідними органами
Недостатня увага до проблем безпеки в інформативному просторі на рівні вищих керівництв [6]	Недооцінка серйозності кіберзагроз та недостатня фінансова підтримка для захисту	Підвищення свідомості та освіти керівництва, розробка та реалізація стратегій кібербезпеки на рівні держави

При визначенні ключових проблем та викликів перед нормативно-правовими механізмами публічного управління інформаційною безпекою варто врахувати низку факторів, які впливають на цей процес. По-перше, однією з основних проблем є постійна еволюція технологій та загроз у інформативному просторі, що ускладнює завдання підтримки актуального та ефективного законодавства в цій області. Нові методи атак та інциденти в сфері кібербезпеки постійно змінюються, вимагаючи постійного оновлення правових норм і стандартів.

Друга проблема полягає у глобальному характері кіберзагроз та необхідності співпраці між державами у вирішенні цих питань. Це може бути

складним завданням через різницю у правових системах та підходах до захисту інформації. Окрім того, недостатній рівень усвідомлення загроз кібербезпеки та неадекватна реакція на них з боку державних органів можуть також вважатися ключовими проблемами. Важливо також враховувати проблему забезпечення відповідності правових норм реальним потребам та викликам у сфері інформаційної безпеки. Це може включати недоліки у законодавстві, які не враховують нові вектори атак або недостатньо чітко визначають обов'язки та відповідальність сторін. Усунення цих проблем потребує спільних зусиль урядовців, експертів з кібербезпеки та законодавців для розробки та впровадження ефективних правових механізмів, які відповідали б сучасним викликам у цій сфері – рис. 1.

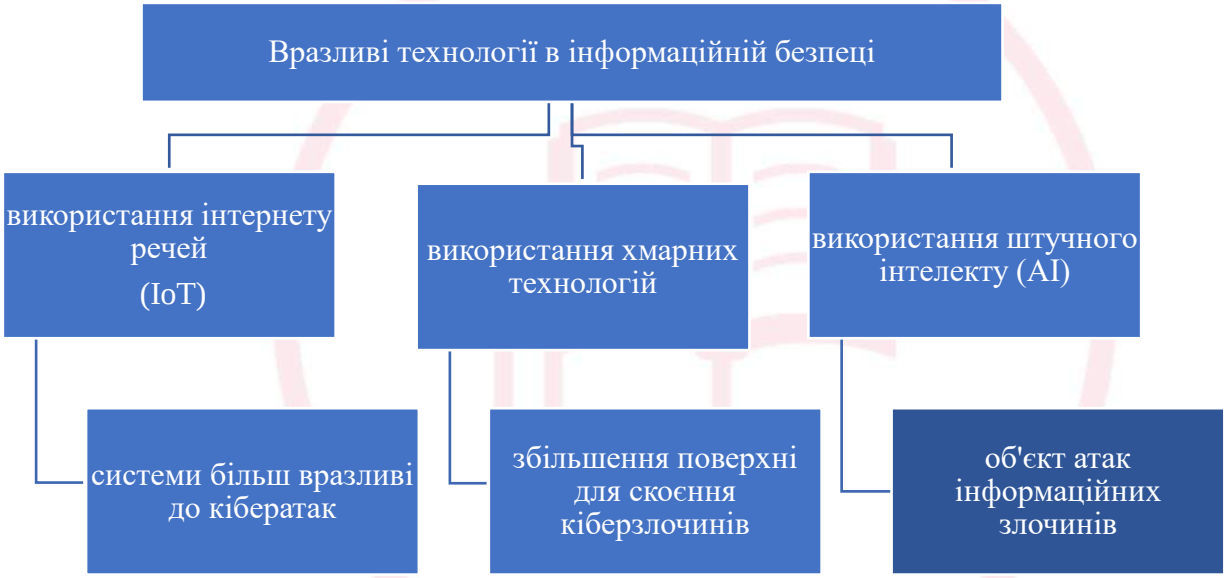

Рис.1. Нові виклики у сфері інформаційної безпеки [7]

Важлива тенденція сучасності полягає в зростанні усвідомлення користувачів щодо кібербезпеки та їх прагнення захищати свої дані. Зміна свідомості користувачів та підвищення вимог до захисту приватності може сприяти вдосконаленню методів захисту інформації та зниженню ризиків [8].

Однак, разом з цими позитивними тенденціями, існують і виклики. Наприклад, розподілені команди та робота на відстані ускладнюють моніторинг та управління інформаційною безпекою, а також збільшують ризик неавторизованого доступу.

Загалом, розуміння сучасних трендів та тенденцій у цифровому середовищі дозволяє краще розуміти загрози та виклики, які стоять перед ефективним захистом інформації. Враховуючи ці фактори, можна розробити більш адаптивні та ефективні стратегії захисту інформації, що відповідають сучасним умовам та потребам користувачів. Підвищення рівня інформаційної

безпеки у сфері надання електронних послуг вимагає постійного вдосконалення законодавства та регуляторних механізмів, які регулюють цю діяльність [9].

Однією з можливостей для вдосконалення є удосконалення правового регулювання щодо захисту персональних даних та конфіденційної інформації. Це може включати в себе введення більш жорстких вимог до організацій, що збирають та обробляють особисту інформацію, а також збільшення відповідальності за порушення правил обробки особистих даних. Крім того, важливо розглядати можливості для створення стандартів безпеки та сертифікації для систем та сервісів, що використовуються в сфері електронних послуг, що дозволить користувачам легше визначати безпечні та надійні сервіси, а також збільшить впевненість у безпеці їхніх даних. Також важливим є удосконалення механізмів контролю та нагляду за дотриманням законодавства щодо кібербезпеки, що може включати в себе збільшення ролі спеціалізованих органів з регулювання інформаційної безпеки, а також розширення їхніх повноважень та ресурсів для ефективнішого контролю за діяльністю суб'єктів, які надають електронні послуги. Крім того, важливо сприяти розвитку культури інформаційної безпеки серед користувачів електронних послуг шляхом проведення освітніх кампаній та навчання населення базовим принципам захисту своєї інформації, що може включати в себе організацію семінарів, вебінарів та інших форм навчання з питань безпеки в інформативному просторі, зокрема у сфері надання електронних послуг [10].

Загалом, виявлення та впровадження можливостей для вдосконалення законодавства та регуляторних механізмів в сфері надання електронних послуг є важливим кроком у підвищенні рівня інформаційної безпеки та забезпеченні довіри користувачів до цифрових сервісів [11].

Отже, на основі аналізу публічного управління інформаційної безпеки у сфері надання електронних послуг можна сформулювати конкретні рекомендації для подальшого вдосконалення нормативно-правових механізмів:

1. Проведення регулярних оновлень законодавства з урахуванням останніх технологічних та інформаційно безпечних тенденцій.
2. Встановлення жорстких вимог до захисту персональних даних та конфіденційної інформації, включаючи введення штрафів за порушення цих вимог.
3. Стимулювання розвитку стандартів безпеки та сертифікації для продуктів та послуг, що використовуються в сфері інформаційної безпеки.
4. Збільшення ролі та повноважень спеціалізованих органів з регулювання кібербезпеки та забезпечення їх належного фінансування.

5. Організація освітніх кампаній та навчання з питань кібербезпеки для споживачів електронних послуг та фахівців.

6. Підтримка міжнародного співробітництва та обміну інформацією між державами з метою виявлення та протидії кіберзагрозам.

7. Проведення аудитів та перевірок щодо дотримання законодавства з питань кібербезпеки в організаціях, що надають електронні послуги.

8. Забезпечення регулярного моніторингу та аналізу ситуації з кібербезпекою для своєчасного реагування на нові загрози та виклики.

9. Сприяння розробці та впровадженню нових технологій та інновацій для підвищення рівня інформаційної безпеки.

10. Взаємодія з приватним сектором та громадськими організаціями для спільного вирішення питань кібербезпеки та вдосконалення законодавства відповідно до потреб суспільства.

Висновки. Проведений аналіз сучасного стану нормативно-правових механізмів публічного управління захистом інформаційної безпеки у сфері надання електронних послуг свідчить про існуючі прогалини та недоліки у цій сфері. Насамперед, виявлено, що відсутність єдиного підходу та координації між органами управління сприяє розпаду зусиль та знижує ефективність заходів з кібербезпеки. Визначені ключові проблеми та виклики перед нормативно-правовими механізмами публічного управління інформаційною безпекою вказують на необхідність невідкладних заходів для забезпечення безпеки електронних послуг. Зокрема, встановлені проблеми недостатньої правової бази, браку спеціалізованих кадрів та недооцінки серйозності кіберзагроз на вищих рівнях управління. Проаналізовані сучасні тренди та тенденції у цифровому середовищі свідчать про постійну еволюцію інформативних загроз та зміну підходів до їх протидії. Зростання кількості зв'язаних пристроїв, використання хмарних технологій та розширення застосування штучного інтелекту вимагають постійного оновлення та адаптації правового регулювання. Виявлені можливості для вдосконалення законодавства та регуляторних механізмів управління інформаційною безпекою відкривають перспективи для підвищення рівня захисту електронних послуг. Серед них - розробка нових законодавчих актів, створення стандартів безпеки та сприяння розвитку спеціалізованих кадрів. Розроблені рекомендації для подальшого вдосконалення нормативно-правових механізмів управління інформаційною безпекою покликані сприяти покращенню системи захисту електронних послуг у контексті сучасних викликів та тенденцій. Їх виконання може допомогти забезпечити більшу безпеку та довіру користувачів до цифрових сервісів.

Література:

1. Дикий, А. П., Дика, О. С., Наумчук, К. М., Тростенюк, Т. М. (2022). ПОНЯТІЙНО-КАТЕГІОРІАЛЬНИЙ АПАРАТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ. *Таврійський науковий вісник.* Серія: Публічне управління та адміністрування, (4), 23-31. https://doi.org/10.32851/tnv-pub.2022.4.3 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

2. Rajvanshi, P.R., Singh, T., Gupta, D. and Gupta, M. (2022), "Cybersecurity and Data Privacy in the Insurance Market", Sood, K., Balusamy, B., Grima, S. and Marano, P. (Ed.) *Big Data Analytics in the Insurance Market (Emerald Studies in Finance, Insurance, and Risk Management)*, Emerald Publishing Limited, Leeds, pp. 1-20. https://doi.org/10.1108/978-1-80262-637-720221001 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

3. Khan, F. and Mer, A. (2023), "Embracing Artificial Intelligence Technology: Legal Implications with Special Reference to European Union Initiatives of Data Protection", Sood, K., Balusamy, B. and Grima, S. (Ed.) *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management* (*Contemporary Studies in Economic and Financial Analysis, Vol. 111C*), Emerald Publishing Limited, Leeds, pp. 119-141. https://doi.org/10.1108/S1569-37592023000111C007 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

4. Rangu, C.M., Badea, L., Scheau, M.C., Găbudeanu, L., Panait, I. and Radu, V. (2024), "Cyber insurance risk analysis framework considerations", *Journal of Risk Finance*, Vol. 25 No. 2, pp. 224-252. https://doi.org/10.1108/JRF-10-2023-0245 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

5. Saritepeci, M., Yildiz Durak, H., Özüdoğru, G. and Atman Uslu, N. (2024), "The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender", *Online Information Review*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/OIR-03-2023-0122 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

6. Spagnolo, M., Ndou, V., Giribaldi, D. and Arena, V. (2023), "A Framework for Dealing With Cybersecurity Risks as Part of Information Security", Akkaya, B., Apostu, S.A., Hysa, E. and Panait, M. (Ed.) *Digitalization, Sustainable Development, and Industry 5.0*, Emerald Publishing Limited, Leeds, pp. 101-123. https://doi.org/10.1108/978-1-83753-190-520231007 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

7. Amonoo Nkrumah, B., Qian, W., Kaur, A. and Tilt, C. (2023), "Stakeholder accountability in the era of big data: an exploratory study of online platform companies", *Qualitative Research in Accounting & Management*, Vol. 20 No. 4, pp. 447-484. https://doi.org/10.1108/QRAM-03-2022-0042 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

8. Göksan, G. (2023), "Digitalization in Public Administration", Akkaya, B. and Tabak, A. (Ed.) *Two Faces of Digital Transformation*, Emerald Publishing Limited, Leeds, pp. 47-57. https://doi.org/10.1108/978-1-83753-096-020231004 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

9. Lyon, G. (2023), "Informational inequality: the role of resources and attributes in information security awareness", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-04-2023-0063 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

10. Nawafleh, S. and Khasawneh, A. (2024), "Drivers of citizens E- loyalty in E-government services: E-service quality mediated by E-trust based on moderation role by system anxiety", *Transforming Government: People, Process and Policy*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TG-04-2023-0053 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

11. Špaček, D. and Špačková, Z. (2023), "Issues of e-government services quality in the digital-by-default era – the case of the national e-procurement platform in Czechia", *Journal of Public Procurement*, Vol. 23 No. 1, pp. 1-34. https://doi.org/10.1108/JOPP-02-2022-0004 (відкритий доступ, дата звернення 25.03.2024, назва з екрану)

References:

1. Dykyi, A. P., Dyka, O. S., Naumchuk, K. M., & Trosteniuk, T. M. (2022). PONIATIINO-KATEHIORIALNYI APARAT INFORMATSIINOI BEZPEKY UKRAINY V ZABEZPECHENNI NATSIONALNOI BEZPEKY [CONCEPTUAL AND CATEGORICAL APPARATUS OF INFORMATION SECURITY OF UKRAINE IN ENSURING NATIONAL SECURITY]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia / Taurian Scientific Herald.* Series: Public management and administration, (4), 23-31. https://doi.org/10.32851/tnv-pub.2022.4.3 [in Ukrainian]

2. Rajvanshi, P.R., Singh, T., Gupta, D. and Gupta, M. (2022), "Cybersecurity and Data Privacy in the Insurance Market", Sood, K., Balusamy, B., Grima, S. and Marano, P. (Ed.) *Big Data Analytics in the Insurance Market (Emerald Studies in Finance, Insurance, and Risk Management)*, Emerald Publishing Limited, Leeds, pp. 1-20. https://doi.org/10.1108/978-1-80262-637-720221001 [in English]

3. Khan, F. and Mer, A. (2023), "Embracing Artificial Intelligence Technology: Legal Implications with Special Reference to European Union Initiatives of Data Protection", Sood, K., Balusamy, B. and Grima, S. (Ed.) *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management* (*Contemporary Studies in Economic and Financial Analysis, Vol. 111C*), Emerald Publishing Limited, Leeds, pp. 119-141. https://doi.org/10.1108/S1569-37592023000111C007 [in English]

4. Rangu, C.M., Badea, L., Scheau, M.C., Găbudeanu, L., Panait, I. and Radu, V. (2024), "Cyber insurance risk analysis framework considerations", *Journal of Risk Finance*, Vol. 25 No. 2, pp. 224-252. https://doi.org/10.1108/JRF-10-2023-0245 [in English]

5. Saritepeci, M., Yildiz Durak, H., Özüdoğru, G. and Atman Uslu, N. (2024), "The role of digital literacy and digital data security awareness in online privacy concerns: a multi-group analysis with gender", *Online Information Review*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/OIR-03-2023-0122 [in English]

6. Spagnolo, M., Ndou, V., Giribaldi, D. and Arena, V. (2023), "A Framework for Dealing With Cybersecurity Risks as Part of Information Security", Akkaya, B., Apostu, S.A., Hysa, E. and Panait, M. (Ed.) *Digitalization, Sustainable Development, and Industry 5.0*, Emerald Publishing Limited, Leeds, pp. 101-123. https://doi.org/10.1108/978-1-83753-190-520231007 [in English]

7. Amonoo Nkrumah, B., Qian, W., Kaur, A. and Tilt, C. (2023), "Stakeholder accountability in the era of big data: an exploratory study of online platform companies", *Qualitative Research in Accounting & Management*, Vol. 20 No. 4, pp. 447-484. https://doi.org/10.1108/QRAM-03-2022-0042 [in English]

8. Göksan, G. (2023), "Digitalization in Public Administration", Akkaya, B. and Tabak, A. (Ed.) *Two Faces of Digital Transformation*, Emerald Publishing Limited, Leeds, pp. 47-57. https://doi.org/10.1108/978-1-83753-096-020231004 [in English]

9. Lyon, G. (2023), "Informational inequality: the role of resources and attributes in information security awareness", *Information and Computer Security*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-04-2023-0063 [in English]

10. Nawafleh, S. and Khasawneh, A. (2024), "Drivers of citizens E- loyalty in E-government services: E-service quality mediated by E-trust based on moderation role by system anxiety", *Transforming Government: People, Process and Policy*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/TG-04-2023-0053 [in English]

11. Špaček, D. and Špačková, Z. (2023), "Issues of e-government services quality in the digital-by-default era – the case of the national e-procurement platform in Czechia", *Journal of Public Procurement*, Vol. 23 No. 1, pp. 1-34. https://doi.org/10.1108/JOPP-02-2022-0004 [in English]