Філософія, методологія, теорія та історія
основ національної безпеки держави

УДК 351

Богоніс Андрій Ростиславович
аспірант кафедри публічного адміністрування
Міжрегіональної Академії управління персоналом
Bogonis Andrii
Postgraduate Student of the Department of Public Administration
Interregional Academy of Personnel Management
ORCID: 0009-0000-6284-4098

ДЕРЖАВНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ: НОВІ ВИКЛИКИ ПРИ ПОСИЛЕННІ ЗАГРОЗ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ
STATE MANAGEMENT OF INFORMATION SECURITY: NEW CHALLENGES AMID HEIGHTENED THREATS TO NATIONAL SECURITY

Анотація. *Вступ. Доведено, що забезпечення інформаційної безпеки критично важливе для України, особливо у зв'язку з її геополітичним становищем та триваючою війною. Інформаційна безпека сьогодні є синонімом національної безпеки для країни. У зв'язку з повномасштабним вторгненням, захист конфіденційних даних, які стосуються військової тактики та стратегії, стає вирішальним, щоб не дати противникам отримати тактичну перевагу.*

Метою дослідження є характеристика особливостей державного управління інформаційною безпекою в умовах нових викликів й загроз. Визначено, що ефективні заходи інформаційної безпеки виявилися необхідними для захисту критично важливих систем від зламів і забезпечення безперервності урядових та військових операцій.

Інформаційна безпека також визначена як ключ до економічної стабільності, оскільки економіка України значно оцифрована і спирається на безпечну кіберінфраструктуру.

Результати. Встановлено, що в умовах зростаючих кіберзагроз уряд України переглянув своє законодавство та політику в галузі кібербезпеки. Ці реформи спрямовані на підвищення стійкості критично важливих інфраструктур і посилення правил інформаційної безпеки у різних секторах. Суворіші покарання за шкідливу кібердіяльність також встановлено для стримування потенційних кіберзлочинців та суб'єктів, які спонсорують держави.

Висновки. Доведено, що у відповідь на кіберзагрози, держава активізувала співпрацю з приватним сектором через державно-приватні партнерства. Це сприяло використанню технічного досвіду та інноваційних можливостей приватних компаній для зміцнення національних систем кібербезпеки. Спільна відповідальність за аналіз загроз, дослідження та розробки у галузі технологій кібербезпеки є важливою. Програми освіти та підвищення обізнаності стали пріоритетом для зниження ризику кіберзламів через недбалість або відсутність знань. Національні кампанії та програми навчання допомагають інформувати громадян про передові методи захисту даних та важливість дотримання протоколів безпеки.

Ключові слова: *державне управління, інформація, інформаційна сфера, державна політика, інформаційна безпека*

Summary. *Introduction. It has been proven that ensuring information security is critically important for Ukraine, especially given its geopolitical position and the ongoing war. Today, information security is synonymous with national security for the country. With the full-scale invasion, protecting*

confidential data related to military tactics and strategy becomes crucial to prevent adversaries from gaining a tactical advantage.

Purpose. The objective of this study is to characterize the peculiarities of state management of information security amid new challenges and threats. It has been determined that effective information security measures are necessary to protect critical systems from breaches and ensure the continuity of government and military operations. Information security is also identified as key to economic stability, as Ukraine's economy is highly digitized and relies on a secure cyber infrastructure. In response to escalating cyber threats, the Ukrainian government has reviewed its legislation and policies in the field of cybersecurity.

Results. These reforms are aimed at enhancing the resilience of critical infrastructures and strengthening information security regulations across various sectors. Stricter punishments for harmful cyber activities have also been established to deter potential cybercriminals and state-sponsored actors. It has been proven that in response to cyber threats, the state has activated cooperation with the private sector through public-private partnerships.

Conclusions. This has facilitated the use of technical expertise and innovative capabilities of private companies to strengthen national cybersecurity systems. Joint responsibility for threat analysis, research, and development in cybersecurity technologies is important. Education and awareness programs have become a priority to reduce the risk of cyber breaches due to negligence or lack of knowledge. National campaigns and training programs help inform citizens about advanced data protection methods and the importance of adhering to security protocols. Summing up, it should be emphasized that in wartime conditions, the goal of information security in Ukraine is crucial for several comprehensive strategic and operational reasons.

Key words: *state management, information, information sphere, state policy, information security*

Постановка проблеми. Забезпечення інформаційної безпеки критично важливе для України, особливо у зв'язку з її геополітичним становищем та війною, що досі триває. При цьому, саме для України інформаційна безпека сьогодні, є синонімом національної безпеки. Внаслідок повномасштабного вторгнення, захист конфіденційних даних має вирішальне значення. Інформація, що стосується військової тактики, позицій та стратегії, має бути захищена, щоб не дати противникам отримати тактичну перевагу. Кібервійна стала інструментом сучасної війни, а Україна стала головною мішенню для кібератак, спрямованих на підрив її військових операцій та державних функцій. Ефективні заходи інформаційної безпеки необхідні захисту цих критично важливих систем від зламів і забезпечення безперервності урядових і військових операцій. Інформаційна безпека є також ключем до забезпечення економічної стабільності. Економіка України сильно оцифрована, і значна частина її економічної діяльності спирається на безпечну та стійку до відмови кіберінфраструктуру. Кібератаки, націлені на критично важливу інфраструктуру, таку як енергопостачання, банківські системи та державні послуги, можуть призвести до значних економічних потрясінь. Захист цих систем від кіберзагроз має вирішальне значення для запобігання фінансовим втратам і підтримці довіри інвесторів, що особливо важливо для країни, що прагне економічного відновлення і зростання в умовах війни. Оскільки Україна продовжує тісніше співпрацювати із західними країнами, забезпечення високих стандартів інформаційної безпеки стає передумовою для більш глибокої інтеграції у глобальні мережі. Дотримання міжнародних стандартів та практик кібербезпеки не лише підвищує авторитет України, а й зміцнює довіру з боку міжнародних партнерів та союзників. Ця довіра має важливе значення для співпраці у сфері оборони, торгівлі та дипломатії, допомагаючи Україні отримати необхідну підтримку та створити стратегічні альянси.

Аналіз останніх досліджень і публікацій. Важливі аспекти забезпечення інформаційної безпеки розкривалися в роботах таких вчених, як M. Johnson [1], K. Thompson [2], E. Wilson [3], V. Edwards [4], G. Brooks [5], Y. Wallace [6], М. Б. Кулинич [7], О. Охріменко [8], І. Б. Шевчук [9], L. Morgan [10] та ін. Однак низка теорій і концепцій в контексті нових викликів національній безпеці в системі державного управління, досі залишаються не розкритими повною мірою, що й зумовило вибір даної тематики, її сучасну актуальність.

Метою дослідження є характеристика особливостей державного управління інформаційною безпекою в умовах нових викликів й загроз.

Виклад основного матеріалу. Інформаційна безпека – це захист даних, що включає процеси, інструменти та політику, необхідні для запобігання, виявлення, документування та протидії загрозам цифрової та фізичної інформації [1-3]. Національна інформаційна безпека є найважливішим компонентом апарату безпеки країни, гарантуючи, що інформаційні ресурси як державного, так і приватного сектора захищені від шпигунства, крадіжки та саботажу [4-5]. Цілісність, конфіденційність та доступність інформації мають важливе значення для підтримки економічної стабільності, громадської безпеки та національної безпеки країни. При цьому, втручання держави в інформаційну безпеку має вирішальне значення через складний характер загроз, для боротьби з якими поодинці приватні підприємства можуть бути погано підготовлені. Держава має унікальні регулюючі можливості для забезпечення дотримання стандартів, проведення спостереження та накладення штрафів, які можуть стримувати або пом'якшувати кіберзагрози [6-10]. Більше того, проблеми національної безпеки потребують координації між різними секторами та відомствами, а ефективно організувати це може лише держава. Такий централізований підхід дозволяє забезпечити більш

ефективний та скоординований захист від міжнародних кіберзагроз та атак (рис. 1).

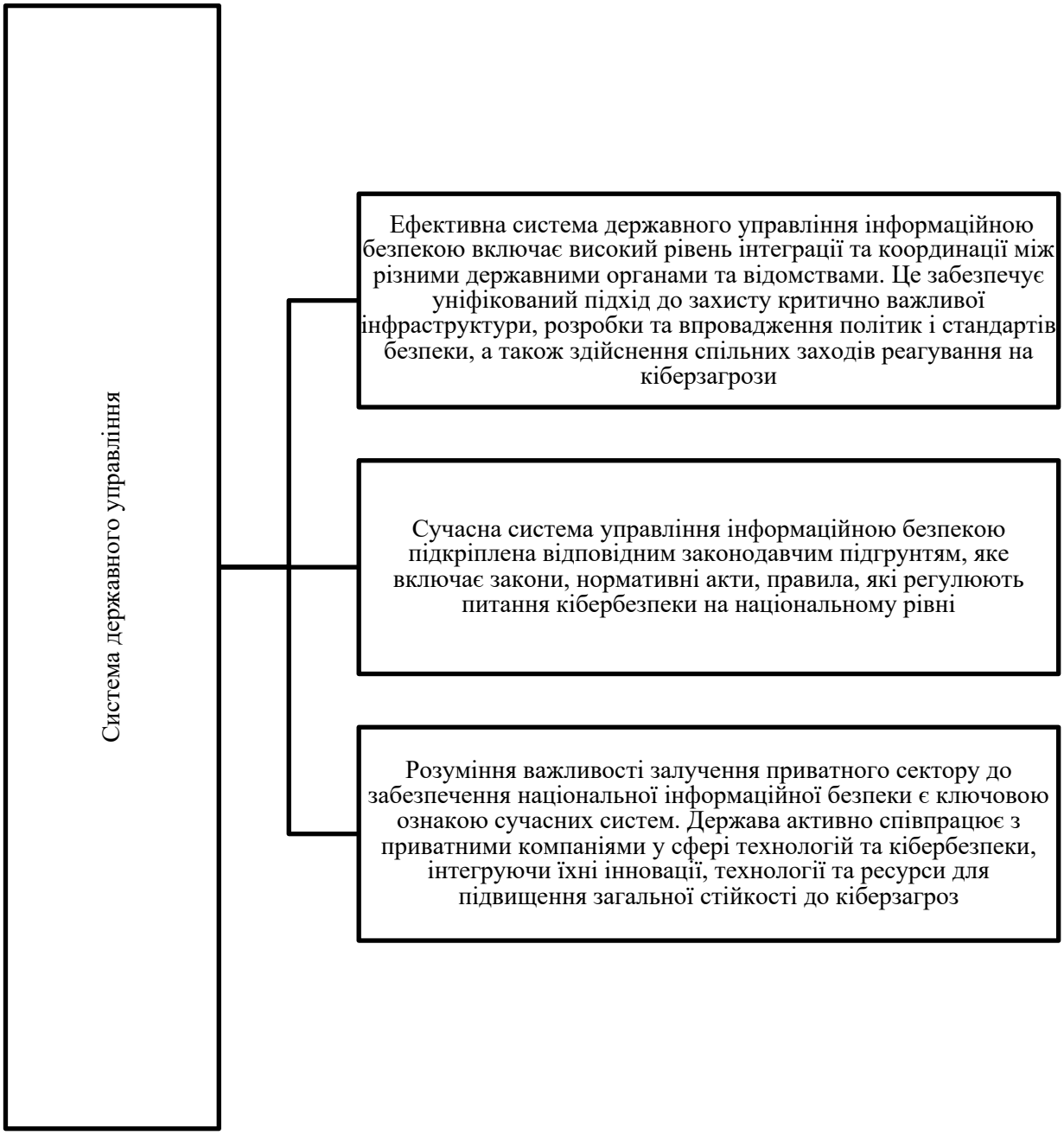

Рис. 1. Характеризуючі ознаки сучасної системи державного управління інформаційною безпекою

Джерело: розроблено автором

Початок війни в Україні у 2022 році ознаменував значну ескалацію тактики кібервійни, висунувши на перший план уразливості у національних та міжнародних системах інформаційної безпеки. У цей

період спостерігалося зростання кібератак, спрямованих на руйнування критичної інфраструктури, крадіжку конфіденційних даних та поширення дезінформації. Цю діяльність часто приписують суб'єктам, які спонсорують держава, що підкреслює геополітичний вимір кібербезпеки. У відповідь на ці загрози, що зросли, держава прийняли кілька стратегій щодо зміцнення своєї інформаційної безпеки під час війни. До них належать посилення протоколів кібербезпеки, розширення обміну розвідданими між союзниками та інвестиції у передові технології кібербезпеки. Уряди України також працював над розширенням своїх кіберзахисних можливостей, прагнучи як захистити власні цифрові активи, так і стримувати противників за допомогою кіберрозвідки і контрзаходів.

Щоб впоратися зі змінною кіберзагроз, уряд переглянув своє законодавство та політику в галузі кібербезпеки. Ці реформи спрямовані на підвищення стійкості критично важливих інфраструктур, покращення можливостей реагування на інциденти та посилення правил щодо практики інформаційної безпеки у різних секторах. Такі законодавчі заходи також спрямовані на суворіше покарання за шкідливу кібердіяльність, тим самим стримуючи потенційних кіберзлочинців та суб'єктів, які держава спонсорує. Визнаючи роль приватного сектору у національній кібербезпеці, держава все активніше бере участь у державно-приватному партнерстві. Метою такого співробітництва є використання технічного досвіду та інноваційних можливостей приватних компаній для зміцнення національних систем кібербезпеки. Такі партнерства часто передбачають спільну відповідальність за аналіз загроз, дослідження та розробки в галузі технологій кібербезпеки, а також реалізацію спільних стратегій реагування під час кіберінцидентів (рис. 2).

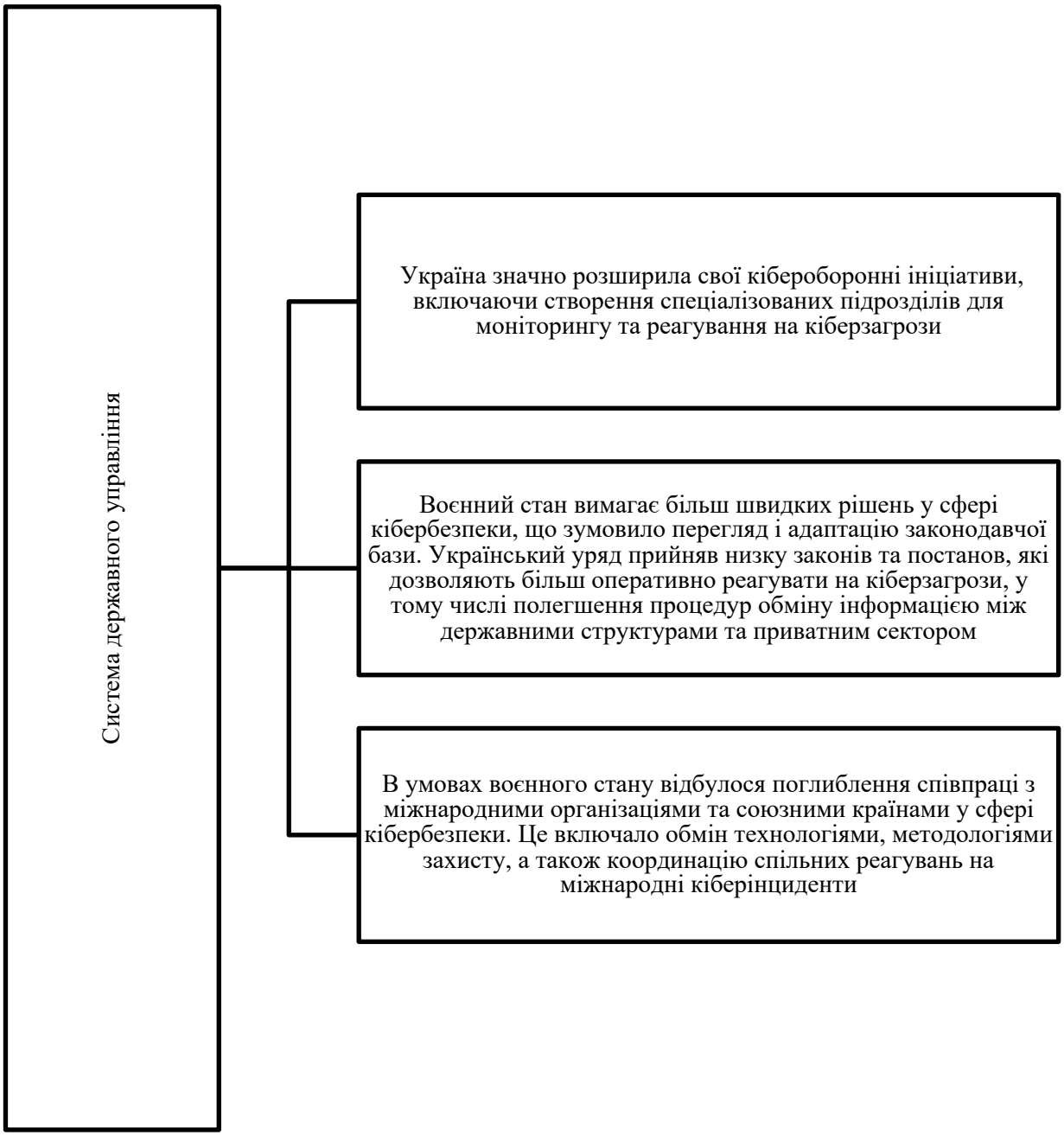

Рис. 2. Ключові зміни в системі державного управління інформаційною безпекою під впливом воєнного стану

Джерело: розроблено автором

Оскільки людські помилки є серйозною вразливістю у сфері кібербезпеки, Україна приділяє пріоритетну увагу програмам освіти та підвищення обізнаності як для державного, так і для приватного секторів. Ці програми призначені для інформування окремих осіб та організацій про передові методи захисту даних, розпізнавання загроз та важливість

дотримання протоколів безпеки. Освітні ініціативи часто підтримуються національними кампаніями та програмами навчання, спрямованими на зниження кількості кіберзламів через недбалість або відсутність знань.

Висновки. Підсумовуючи слід наголосити, що в умовах воєнного часу мета інформаційної безпеки в Україні має вирішальне значення з кількох всеосяжних стратегічних та оперативних причин. Це відображає відданість захисту національних інтересів, захисту життя цивільного населення та забезпечення стабільності та безперервності функцій уряду. Кібератаки можуть бути спрямовані на ці мережі, щоб спричинити збої, вкрасти конфіденційну інформацію та підірвати можливості національної оборони. Ефективні заходи інформаційної безпеки гарантують, що збройні сили можуть діяти безкомпромісно, а критично важливі системи, такі як енергетика, зв'язок та транспорт, захищені від перешкод, що має першорядне значення для підтримки оборонної готовності та безперервності операцій під час війни. Оскільки інфраструктури все частіше зазнають кібератаки, ризик витоку персональних даних зростає. Для українців безпека особистої інформації — це не лише питання конфіденційності, а й безпеки, оскільки виток даних може піддати громадян цілеспрямованим атакам і експлуатації. Надійні протоколи інформаційної безпеки необхідні для запобігання таким порушенням та забезпечення конфіденційності та безпеки особистих даних у періоди активних військових дій.

Література

1. Johnson M. K., Parker T. J., Smith A. C., Benson O. L., Lewis L. S. Enhancing Cyber Defense Capabilities in Public Sector Networks: A U.S. Perspective. *Journal of Information Security and Applications.* 2020. 16(1). P. 115-126.

2. Thompson K. V., Reynolds M. O., Harper J. A., Collins P. V., Young Y. L. Data Protection Strategies in Healthcare: Learning from Recent Breaches. *American Journal of Healthcare Management.* 2020. 14(3). P. 202-215.

3. Wilson E. A., Green C. K., Carter D. M., Hill S. P., Mitchell L. M. Secure Digital Identity Verification Techniques and Their Impact on National Security. *Journal of Cyber Policy and Governance*. 2021. 25(4). P. 480-498.

4. Edwards V. I., Anderson M. I., Lawson O. V., Perry I. M., Stuart P. S. The Role of Artificial Intelligence in Enhancing Cybersecurity: Opportunities and Challenges. *Technology and Security Review*. 2021. 20(2). P. 134-152.

5. Brooks G. I., Kennedy V. P., Watson M. L., Foster O. Y., Chase M. O. Protecting Financial Infrastructures from Cyber-Physical Threats: A Case Study Approach. *Journal of Financial Information Security*. 2022. 12(1). P. 88-102.

6. Wallace Y. V., Phelps C. M., Lawson R. I., Hamilton S. G., Grant V. G. Blockchain as a Tool for Transparency and Security in Public Administration. *Journal of Technology in Governance.* 2022. 9 (4). P. 310–328.

7. Кулинич М. Б., Матвійчук І. О., Сафарова А. Т., Герасименко Т. О. Діджиталізація обліку, аналізу та оподаткування в системі управління підприємством. *Вісник Львівського торговельно-економічного університету.* 2021. Вип. 64. С. 57-63.

8. Охріменко О., Іванова т. Соціальна відповідальність : навч. посіб. Київ : Нац. техн. ун-т України «Київ. політехн. ін-т», 2018. 180 с.

9. Шевчук І. Б. Інформаційні технології в регіональній економіці: теорія і практика впровадження та використання : монографія. Львів : АТБ, 2018. 448 с.

10. Morgan L. S., Powell L. V., Nelson D. A., Graham O. E., Knox D. N. Predictive Analytics for Cyber Threat Detection: Enhancing Proactive Measures in the Defense Sector. *Artificial Intelligence and Public Sector Applications.* 2023. 6(2). P. 213-235.

References

1. Johnson, M. K., Parker, T. J., Smith, A. C., Benson, O. L., & Lewis, L. S. (2020). Enhancing Cyber Defense Capabilities in Public Sector Networks: A U.S. Perspective. *Journal of Information Security and Applications,* 16(1), 115-126.

2. Thompson, K. V., Reynolds, M. O., Harper, J. A., Collins, P. V., & Young, Y. L. (2020). Data Protection Strategies in Healthcare: Learning from Recent Breaches. *American Journal of Healthcare Management,* 14(3), 202-215.

3. Wilson, E. A., Green, C. K., Carter, D. M., Hill, S. P., & Mitchell, L. M. (2021). Secure Digital Identity Verification Techniques and Their Impact on National Security. *Journal of Cyber Policy and Governance,* 25(4), 480-498.

4. Edwards, V. I., Anderson, M. I., Lawson, O. V., Perry, I. M., & Stuart, P. S. (2021). The Role of Artificial Intelligence in Enhancing Cybersecurity: Opportunities and Challenges. *Technology and Security Review,* 20(2), 134-152.

5. Brooks, G. I., Kennedy, V. P., Watson, M. L., Foster, O. Y., & Chase, M. O. (2022). Protecting Financial Infrastructures from Cyber-Physical Threats: A Case Study Approach. *Journal of Financial Information Security,* 12(1), 88-102.

6. Wallace, Y. V., Phelps, C. M., Lawson, R. I., Hamilton, S. G., & Grant, V. G. (2022). Blockchain as a Tool for Transparency and Security in Public Administration. *Journal of Technology in Governance,* 9(4), 310-328.

7. Kulynych, M. B., Matviichuk, I. O., Safarova, A. T., & Herasymenko, T. O. (2021). Didzhytalizatsiia obliku, analizu ta opodatkuvannia v systemi upravlinnia pidpryiemstvom [Digitalization of accounting, analysis and taxation in the enterprise management system.]. *Visnyk Lvivskoho torhovelno-ekonomichnoho universytetu – Bulletin of Lviv University of Trade and Economics,* 64, 57-63 [in Ukrainian].

8. Okhpimenko, O., & Ivanova, T. (2018). Socialna vidpovidalnist [Social Responsibility]. Kyiv [in Ukrainian].

9. Shevchuk, I. B. (2018). Informatsiini tekhnolohii v rehionalnii ekonomitsi: teoriia i praktyka vprovadzhennia ta vykoryctannia [Information technologies in the regional economy: theory and practice of implementation and use]: monohpafiia. Lviv: ATB [in Ukrainian].

10. Morgan, L. S., Powell, L. V., Nelson, D. A., Graham, O. E., & Knox, D. N. (2023). Predictive Analytics for Cyber Threat Detection: Enhancing Proactive Measures in the Defense Sector. *Artificial Intelligence and Public Sector Applications,* 6(2), 213-235.