УДК 351
DOI: 10.35432/tisb312024306534

Андрій Богоніс
аспірант кафедри публічного адміністрування
Міжрегіональна Академія управління персоналом, Київ
https://orcid.org/0009-0000-6284-4098
e-mail: bogonis.andrii@gmail.com

ВПЛИВ ЦИФРОВІЗАЦІЇ НА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: НОВІ ЗАГРОЗИ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ

Дослідження присвячене характеристиці особливостей впливу цифровізації на забезпечення інформаційної безпеки в системі державного управління. Доведено, що сьогодні значні представники інтелектуальної, політичної та економічної еліти світу активно долучені до формування глобального та європейського інформаційного суспільства. Встановлено, що інформаційні технології та інформаційно-комунікативні системи є ключовими в умовах сучасного цивілізаційного розвитку, виступаючи не лише як важливі елементи для розвитку держави та суспільства, але й як необхідна умова їхньої конкурентоспроможності на глобальному рівні. Інформаційний сектор відіграє провідну роль у реалізації соціальних ініціатив, зміцненні громадянського суспільства та інтеграції у світове співтовариство. Доведено, що ефективність забезпечення інформаційної безпеки вимірюється здатністю підтримувати високий рівень безпеки інформаційної сфери при мінімальних витратах. Різноманіття внутрішніх і зовнішніх інформаційних загроз може порушити стабільність системи державного управління. Інформаційна безпека є індикатором стабільного стану системи державного управління, здатної зберігати ключові функції під час впливу загроз. Визначено, що серед основних завдань системи забезпечення інформаційної безпеки — створення умов для забезпечення інформаційного суверенітету, вдосконалення нормативно-правової бази для розвитку національної інформаційної інфраструктури, впровадження сучасних технологій, забезпечення достовірної інформації та сприяння мас-медіа у боротьбі з корупцією. Також важливим є гарантування конституційного права на свободу слова, доступ до інформації та захист даних від неправомірного втручання державних структур. Доведено, що цифровізація відіграє ключову роль у зміцненні інформаційної безпеки, підвищуючи ефективність, доступність і безпеку державних операцій. Вона сприяє централізації даних, забезпечує моніторинг у реальному часу та впровадження передових методів шифрування. Крім того, цифровізація є потужним інструментом, який може суттєво підвищити стійкість державних інституцій. Вона робить уряди більш стійкими до кіберзагроз, прозорими та підзвітними, а також дає їм можливість ефективно боротися з дезінформацією. Це, в свою чергу, веде до кращого урядування, зміцнення довіри між владою та суспільством та більш стійкого розвитку країни.

Ключові слова: цифровізація, державне управління, інформаційна сфера, інформаційна безпека.

Andrii Bogonis
PhD-student of the Department of Public Administration
Interregional Academy of Personnel Management, Kyiv
https://orcid.org/0009-0000-6284-4098
e-mail: bogonis.andrii@gmail.com

IMPACT OF DIGITIZATION ON INFORMATION SECURITY: NEW THREATS IN THE PUBLIC ADMINISTRATION SYSTEM

The purpose of the study is to characterize the features of the impact of digitalization on ensuring information security in the public administration system. It has been proven that today major representatives of the intellectual, political and economic elite of the world are actively involved in the formation of a global and European information society. It has been established that information technologies and information and communication systems are key in the conditions of modern civilizational development, acting not only as important elements of the development of the state and society, but also as a necessary condition for their competitiveness at the global level. The information sector plays a leading role in the implementation of social initiatives, strengthening civil society and integration into the world community. It has been proven that the effectiveness of information security is measured by the ability to maintain a high level of information security at minimal cost. The variety of internal and external information threats can disrupt the stability of the public administration system. Information security is an indicator of the stable state of the public administration system, capable of maintaining key functions when exposed to threats. It has been determined that among the main objectives of the information security system is the creation of conditions for ensuring information sovereignty, improving the regulatory framework for the development of national information infrastructure, introducing modern technologies, providing reliable information and promoting the media in the fight against corruption. It is also important to guarantee the constitutional right to freedom of speech, access to information and protection of data from undue interference by government agencies. Digitalization has been proven to play a key role in strengthening information security, making government operations more efficient, accessible and secure. It promotes data centralization, provides real-time monitoring and the implementation of advanced encryption methods. Additionally, digitalization improves the resilience of government operations through cyber defense mechanisms and promotes transparency in government processes. Such transparency helps build trust between government and the public, effectively control information, and counter disinformation.

Key words: digitalization, public administration, information sphere, information security.

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими та практичними завданнями. Інформаційна безпека на державному рівні є критичною проблемою в сьогоднішню цифрову епоху, коли інформація та дані відіграють центральну роль у всіх аспектах національної функціональності — від безпеки та управління до економічної життєздатності та суспільного добробуту. Актуальність та доцільність захисту цих даних неможливо переоцінити, враховуючи масштаб та складність загроз, з якими стикаються країни у всьому світі. Слід зазначити, що інформаційна безпека є життєво важливою для захисту національних інтересів. Державні бази даних містять конфіденційну інформацію, пов'язану з національною обороною, критичною інфраструктурою та операціями

внутрішньої безпеки. Будь-яке порушення або несанкціонований доступ до цих даних може поставити під загрозу здатність країни захистити себе або підтримувати суспільну безпеку. При цьому, так звані кіберзагрози, починаючи від хакерських атак і шпигунства з боку ворожих державних суб'єктів і закінчуючи терористичними угрупованнями, що прагнуть підірвати суспільні функції, є серйозними ризиками. Забезпечення надійних заходів кібербезпеки уможливлює захист країни від цих потенційно руйнівних атак. Відомо, що сьогодні, значна частина сучасної економіки є цифровою. Від банківських систем до корпоративних даних тощо велика частина економічної діяльності залежить від цілісності та доступності цифрових систем. Кібератаки можуть призвести до суттєвих фінансових втрат, підірвати довіру інвесторів та підірвати економічну стабільність. Захищаючи інформаційні системи, держави можуть захистити свою економіку від руйнівного впливу кіберзлочинності та забезпечити безпечне середовище для економічного зростання та інвестицій.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і на які спираються автори. Важливі аспекти забезпечення інформаційної безпеки розкривалися в роботах таких вчених, як Барановський О., Бланк І., Буряк П., Волинський Г., Геєць В., Грідчина М., Ковалюк О., Криштанович М., Козоріз М., Кудря Я., Лещук В., Слав'юк Р., Силкін О., Сутормінa В., Шелудько В., Штангрет, М. та ін. Однак низка теорій і концепцій в контексті врахування впливу цифровізації й аспектів державного управління, досі залишаються не розкритими повною мірою, що й зумовило вибір даної тематики, її сучасну актуальність.

Формулювання цілей статті (постановка завдання). Метою дослідження є характеристика особливостей впливу цифровізації на забезпечення інформаційної безпеки в системі державного управління.

Наукова новизна дослідження полягає в тому, що в ньому вперше буде проведено комплексне дослідження особливостей впливу цифровізації на інформаційну безпеку в системі державного управління з урахуванням сучасних тенденцій та викликів.

Теоретична та практична значимість дослідження полягає в тому, що його результати можуть бути використані для вдосконалення системи інформаційної безпеки в системі державного управління, що сприятиме підвищенню рівня захисту інформаційних ресурсів держави.

Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів. Сьогодні в процес створення глобального і європейського інформаційного суспільства активно втягнуті значні представники інтелектуальної, політичної та економічної еліти ведучих країн світу. В умовах сучасного етапу цивілізаційного розвитку, інформаційні технології та інформаційно-комунікативні системи стають ключовими елементами для розвитку суспільства і держави, а також необхідною умовою їх змагань на глобальному рівні [1-2]. Інформаційний сектор може слугувати провідним чинником в реалізації важливих суспільних ініціатив, зміцненні громадянського суспільства та інтеграції у світове співтовариство. Ефективність забезпечення інформаційної безпеки можна визначити через здатність забезпечувати високий рівень безпеки в інформаційній сфері з мінімальними витратами [3-4]. Різноманіття внутрішніх і зовнішніх інформаційних загроз створює умови, що можуть порушити стабільність системи державного управління. Важливо підкреслити, що інформаційна безпека є показником стабільного та стійкого стану системи державного управління, яка здатна зберігати свої ключові функції під час впливу внутрішніх та зовнішніх загроз (табл.1).

Таблиця 1

Характерні ознаки сутності забезпечення інформаційної безпеки

Захист від зовнішніх та внутрішніх загроз	**Підтримка конфіденційності, цілісності та доступності інформації**	**Використання комплексних технічних та організаційних заходів**	**Адаптація до змінюваних умов і загроз**
Забезпечення інформаційної безпеки передбачає активні заходи щодо захисту інформаційних систем та баз даних від несанкціонованого доступу, зловмисних атак, шпигунства та інших форм кіберзлочинності. Це також включає захист від внутрішніх загроз, таких як витік інформації або саботаж з боку співробітників	Три основні цілі інформаційної безпеки включають забезпечення конфіденційності (захист інформації від розголошення стороннім особам), цілісності (захист від несанкціонованих змін) і доступності (забезпечення доступу до інформації легітимним користувачам, коли вони цього потребують)	Забезпечення інформаційної безпеки вимагає комплексного підходу, що включає в себе технічні рішення, такі як шифрування, брандмауери, антивірусне програмне забезпечення, а також організаційні заходи, як-от політики безпеки, процедури аудиту, обучення персоналу і регулярне тестування систем на вразливості	Інформаційна безпека не є статичною; вона вимагає постійного оновлення і адаптації до нових технологій, загроз та методів кібератак. Стратегії безпеки повинні розвиватися, щоб випереджати потенційні загрози і включати новітні технологічні досягнення для ефективного захисту

Джерело: сформовано автором

Ключові завдання цієї системи включають створення умов для гарантування інформаційного суверенітету країни, вдосконалення державного регулювання розвитку інформаційної сфери шляхом впровадження нормативно-правових та економічних механізмів, що сприятимуть розвитку національної інформаційної інфраструктури, введення сучасних технологій, забезпечення надійної інформації в національному та глобальному інформаційних просторах [5-7]. Також до завдань входить сприяння мас-медіа у боротьбі з корупцією, гарантування конституційного права на свободу слова і доступ до інформації, запобігання недозволеному втручанню владних структур у діяльність медіа, забезпечення безпеки усіх елементів системи державного управління, підтримка інформаційно-аналітичних здібностей країни, виконання політики в галузі інформаційної безпеки, моніторинг стану цієї сфери та охорона державної таємниці [8-10].

Сьогодні саме цифровізація відіграє ключову роль у зміцненні інформаційної безпеки держави, відбиваючи її виняткову важливість у сучасну цифрову епоху. Інтегруючи цифрові технології до різних функцій уряду, цифровізація підвищує ефективність, доступність і безпеку державних операцій, роблячи її наріжним каменем сучасного державного управління. Відтак, цифровізація сприяє централізації та систематичній організації

державних даних, що має вирішальне значення для забезпечення інформаційної безпеки. Завдяки впровадженню складних цифрових баз даних та систем управління уряди можуть захистити конфіденційну інформацію від несанкціонованого доступу та кіберзагроз. Така централізація не тільки підвищує цілісність даних, але й забезпечує моніторинг та аналіз у режимі реального часу, що дозволяє оперативно реагувати на потенційні порушення безпеки. Крім того, такі системи призначені для реалізації передових методів шифрування та контролю доступу, що значно підвищує безпеку критично важливих інформаційних інфраструктур (табл.2).

Таблиця 2

Загрози цифровізації, що негативно впливають
на систему державного управління інформаційною безпекою

Кібератаки та зловмисне програмне забезпечення	**Проблеми з конфіденційністю даних**	**Залежність від цифрових інфраструктур та відмова в обслуговуванні**
Зі зростанням залежності від цифрових систем, державні органи стають більш вразливими до кібератак, включаючи атаки з використанням шкідливого програмного забезпечення, фішинг, атаки на відмову в обслуговуванні (DDoS) та інші види кіберзагроз	Цифровізація спричиняє збільшення обсягів збору, зберігання та обробки персональних даних громадян. Це підвищує ризики, пов’язані з приватністю та захистом даних.	Посилення залежності від цифрових систем може створювати ситуації, у яких відмова однієї критичної системи призводить до каскадного збою в багатьох інших системах

Джерело: сформовано автором

Слід зазначити, що цифровізація сприяє стійкості державних операцій за рахунок впровадження надійних механізмів кіберзахисту. Сучасні стратегії інформаційної безпеки передбачають використання автоматизованих систем виявлення загроз, протоколів безпеки на основі штучного інтелекту та безперервний аудит безпеки. Ці інструменти допомагають виявляти вразливості та загрози до того, як вони можуть бути використані, тим самим запобігаючи потенційним збоям у роботі державних служб та захищаючи дані громадян від кібератак.

Роблячи урядові процеси більш видимими та доступними для громадян через цифрові платформи, природно посилюється контроль і нагляд за цими процесами. Така прозорість допомагає зміцнити довіру між урядом та громадськістю, протидіяти корупції та неправомірному використанню даних, а також гарантувати, що обробка інформації відповідає суворим правовим та етичним стандартам. Можна стверджувати, що саме цифровізація сприяє стратегічному поширенню інформації, що є ключовим аспектом інформаційної безпеки. Контролюючи та керуючи потоками інформації цифровими каналами, держави можуть ефективно спілкуватися з громадськістю під час криз, керувати пропагандою та протидіяти дезінформації. Ця здатність швидко і точно розповсюджувати інформацію має вирішальне значення для підтримки громадського порядку та національної

безпеки, особливо в ситуаціях, коли дезінформація може призвести до паніки чи заворушень. Тому держава повинна зберігати пильність та активно оновлювати свою цифрову інфраструктуру та протоколи безпеки. Це передбачає не лише впровадження новітніх технологій, а й розвиток культури кіберінформації та стійкості серед громадян та співробітників.

Висновки з даного дослідження і перспективи подальших розвідок у даному напрямку. Підсумовуючи слід наголосити, що й сам захист приватної інформації громадян є ще одним важливим аспектом інформаційної безпеки на державному рівні. Оскільки уряди все частіше оцифровують свої послуги, особисті дані громадян, включаючи номери соціального страхування, медичні записи та фінансову інформацію, зберігаються у державних базах даних. Порушення цих систем може призвести до крадіжки особистих даних, шахрайства та серйозної втрати суспільної довіри до державних установ. Приділяючи пріоритетну увагу інформаційній безпеці, уряди можуть захистити конфіденційність своїх громадян та зберегти довіру суспільства до своєї діяльності. Більш того, інформаційна безпека має важливе значення для підтримки міжнародного авторитету та довіри. В епоху глобальної взаємопов'язаності країнам часто доводиться обмінюватися конфіденційною інформацією з метою безпеки, торгівлі та дипломатичних цілей. Здатність захистити інформацію має вирішальне значення підтримки функціональних і довірчих міжнародних відносин. Якщо країна не може захистити свої дані, вона ризикує втратити своє становище та вплив на міжнародній арені, що потенційно може призвести до дипломатичної ізоляції чи конфліктів.

На нашу думку, вивчення та забезпечення інформаційної безпеки актуальні сьогодні через характер кіберзагроз, що постійно змінюється. Кіберзлочинці та ворожі країни постійно розробляють нові методи використання уразливостей в інформаційних системах. Підсумовуючи, можна стверджувати, що актуальність інформаційної безпеки на державному рівні включає захист національної безпеки, економічної стабільності, особистої конфіденційності, міжнародного авторитету та готовності до кіберзагроз, що розвиваються. Зважаючи на ці критичні проблеми, тема інформаційної безпеки не лише актуальна, а й необхідна для вивчення та дій сьогодні й в подальшому зокрема.

Література

1. Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., & Lukashuk, L. Optimization of state regulation in the field of safety and security of business: a local approach. Business: Theory and Practice, 24(2), 2023, 613–621.

2 Le, T. M., & Bui, M.-T. Information source and destination choice: mediation of perception of COVID-19 pandemic impacts and perception of destination. Business: Theory and Practice, 23(2), 2022, 266–276.

3. Černius, G., & Birškytė, L. Financial information and management decisions: impact of accounting policy on financial indicators of the firm. Business: Theory and Practice, 21(1), 2020, 48-57

4. Iskajyan, S.O., Kiseleva, I.A., Tramova, A.M., Timofeev, A.G., Mambetova, F.A., Mustaev, M.M. Importance of the information environment factor in assessing a country's economic security in the digital economy. International Journal of Safety and Security Engineering, 12(6), 2022: 691-697

5. Chen JZ, Lim CY, Lobo GJ Does the relation between information quality and capital structure vary with cross-country institutional differences? Journal of International Accounting

Research 15 (3): 2016, 131–156.

6. Yurkiv, Y., & Krasnova, N. Civil Socialization of Youth in the Conditions of the Postmodern Information Society. Postmodern Openings, 12(1), 2021, 74-90.

7. Kravchuk, O., Shoturma, N., Grabina, G., Myloserdna, I., Vedenieiev, V., & Shtelmashenko, A. The Information Revolution in the Post-Industrial Society: Dangers in Political Processes. Postmodern Openings, 13(4), 2022, 113-126.

8. Kryshtanovych, M., Sakhanienko, S., Sylkin, O., Lypovska, S., Purtskhvanidze, O. Information Support of Public Administration in the Conditions of COVID-19. In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, 2022, pp. 290-293

9. Gunasekaran, M., Chandu, T., Daphne, L., Revathi S. Big data security intelligence for healthcare industry 4.0. Cybersecurity for Industry 4.0, 2017, 103-126

10. Milichovský, F., & Hornungová, J. Methodology for the selection of financial indicators in the area of information and communication activities. Business: Theory and Practice, 14(2), 2013, 97-102.

Література

1. Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., & Lukashuk, L. (2023). Optimization of state regulation in the field of safety and security of business: a local approach. Business: Theory and Practice, 24(2), pp. 613–621. [In English]

2. Le, T. M., & Bui, M.-T. (2022). Information source and destination choice: mediation of perception of COVID-19 pandemic impacts and perception of destination. Business: Theory and Practice, 23(2), pp. 266–276. [In English]

3. Černius, G., & Birškytė, L. (2020). Financial information and management decisions: impact of accounting policy on financial indicators of the firm. Business: Theory and Practice, 21(1), pp. 48-57 [In English]

4. Iskajyan, S.O., Kiseleva, I.A., Tramova, A.M., Timofeev, A.G., Mambetova, F.A., & Mustaev, M.M. (2022). Importance of the information environment factor in assessing a country's economic security in the digital economy. International Journal of Safety and Security Engineering, 12(6): pp. 691-697 [In English]

5. Chen JZ, Lim CY, Lobo GJ (2016) Does the relation between information quality and capital structure vary with cross-country institutional differences? Journal of International Accounting Research 15 (3): pp. 131–156. [In English]

6. Yurkiv, Y., & Krasnova, N. (2021). Civil Socialization of Youth in the Conditions of the Postmodern Information Society. Postmodern Openings, 12(1), pp. 74-90. [In English]

7. Kravchuk, O., Shoturma, N., Grabina, G., Myloserdna, I., Vedenieiev, V., & Shtelmashenko, A. (2022). The Information Revolution in the Post-Industrial Society: Dangers in Political Processes. Postmodern Openings, 13(4), pp. 113-126. [In English]

8. Kryshtanovych, M., Sakhanienko, S., Sylkin, O., Lypovska, S., & Purtskhvanidze, O. (2022). Information Support of Public Administration in the Conditions of COVID-19. In 2022 12th International Conference on Advanced Computer Information Technologies (ACIT), Ruzomberok, Slovakia, pp. 290-293 [In English]

9. Gunasekaran, M., Chandu, T., Daphne, L., & Revathi S. (2017) Big data security intelligence for healthcare industry 4.0. Cybersecurity for Industry 4.0, pp. 103-126 [In English]

10. Milichovský, F., & Hornungová, J. (2013). Methodology for the selection of financial indicators in the area of information and communication activities. Business: Theory and Practice, 14(2), pp. 97-102. [In English]