УДК 351.72:004.056.5
DOI https://doi.org/10.51547/ppp.dp.ua/2024.1.10

Нагорняк Михайло Миколайович,
доктор політичних наук, професор,
кафедра управління та бізнес-адміністрування
Прикарпатського національного університету імені Василя Стефаника
ORCID ID: 0000-0001-8947-3450

ІНФОРМАЦІЙНА БЕЗПЕКА У СИСТЕМІ ПУБЛІЧНОГО УПРАВЛІННЯ: ВИКЛИКИ ТА ПЕРСПЕКТИВИ

INFORMATION SECURITY IN THE PUBLIC ADMINISTRATION SYSTEM: CHALLENGES AND PROSPECTS

За останні десятиліття інформаційна безпека у системі публічного управління стала критично важливою в умовах постійного технологічного розвитку та зростання кількості кіберзагроз. Порушення безпеки інформації в органах влади та адміністрації ведуть до серйозних наслідків, включаючи можливість втрати конфіденційної інформації, маніпуляції громадською думкою та загрози національній безпеці. Основна проблема полягає у тому, як ефективно захищати інформаційні ресурси в системі публічного управління в умовах постійно зростаючих технологічних викликів та кіберзагроз. Метою даного дослідження є системний аналіз викликів та перспектив інформаційної безпеки у сфері публічного управління, розробка стратегій захисту та ідентифікація шляхів покращення систем безпеки інформації в державних структурах. Об'єктом дослідження є система публічного управління, а предметом - проблеми, пов'язані із захистом інформаційних ресурсів цієї системи в умовах сучасних технологічних та кібернетичних викликів. У роботі використано аналіз наукової літератури, апробацію на практиці різних методів захисту інформації, а також участь у наукових конференціях та діалозі з провідними фахівцями в галузі. Спеціальний акцент був зроблений на аналізі кейсів кібератак та вивченні досвіду країн, які досягли успіхів у сфері інформаційної безпеки в публічному управлінні. Автор успішно розкрив відомі та нові виклики, що постають перед системою інформаційної безпеки в умовах публічного управління. Здійснив порівняльний аналіз різних підходів до захисту інформації, ідентифікував найбільш ефективні стратегії та методи захисту. Висновки дослідження роблять акцент на необхідності впровадження комплексних заходів, зокрема, посилення ролі відкритих даних, підвищення кваліфікації кадрів та вдосконалення системи моніторингу та реагування на потенційні кіберзагрози. Рекомендації спрямовані на практичне впровадження в органи публічного управління для забезпечення стійкої та ефективної інформаційної безпеки.

Ключові слова: *публічне управління, механізми публічного управління, інформаційна безпека, управління інформаційною безпекою, публічне управління інформаційною безпекою.*

In recent decades, information security in the system of public administration has become critically important in the conditions of constant technological development and the increase in the number of cyber threats. Breaches of information security in government and administration lead to serious consequences, including the possibility of loss of confidential information, manipulation of public opinion and threats to national security. The main problem is how to effectively protect information resources in the public administration system in the conditions of constantly growing technological challenges and cyber threats. The purpose of this research is a systematic analysis of the challenges and prospects of information security in the field of public administration, development of protection strategies and identification of ways to improve information security systems in state structures. The object of research is the system of public management, and the subject is the problems related to the protection of information resources of this system in the conditions of modern technological and cybernetic challenges. The work used the analysis of scientific literature, the practical approbation of various methods of information protection, as well as participation in scientific conferences and dialogue with leading specialists in the field. A special emphasis was placed on the analysis of cases of cyber attacks and the study of the experience of countries that have achieved success in the field of information security in public administration. The author successfully revealed known and new challenges facing the information security system in public administration. Conducted a comparative analysis of various approaches to information protection, identified the most effective protection strategies and methods. The conclusions of the study emphasize the need to implement complex measures, in particular, strengthening the role of open data, improving the qualifications of personnel, and improving the system of monitoring and responding to potential cyber threats. The recommendations are aimed at practical implementation in public administration bodies to ensure sustainable and effective information security.

Key words: *public administration, public administration mechanisms, information security, information security management, public information security management.*

Постановка проблеми. Інформаційна безпека у системі публічного управління стає у сучасному світі критичною проблемою, оскільки супроводжується значними викликами та перспективами. Сучасні тренди та тенденції демонструють, що з кожним роком кількість кіберзагроз зростає, а їх складність та різноманітність викликають серйозні труднощі для забезпечення ефективного функціонування систем управління.

Згідно з останніми статистичними даними, зафіксовано значний приріст кількості кібератак на державні структури. За останні роки спостерігається зростання кількості інцидентів, пов'язаних із неправомірним доступом до конфіденційної інформації, витоками даних та втратами функціональності критичних систем управління. Наприклад, за даними державного центру кіберзахисту державної служби спеціально зв'язку та захисту інформації, лише протягом останнього року кількість кібератак на установи публічного управління зросла на 30%.

З урахуванням вищезазначених викликів та тенденцій, наукова спільнота та владні структури повинні спільно працювати над розробкою та впровадженням нових стратегій та рішень із забезпечення інформаційної безпеки в системах публічного управління.

Аналіз літературних джерел. Актуальність теми дослідження визначається увагою авторів до розробки проблематики, зокрема, . Усик, С., Chen, H., Hai, Y., Citation Tuna, A.A., Türkmendağ, Z., Sun, Y., Zhang, Y. F., Wang, Y., Zhang, S., Дикий, А. П., Дика, О. С., Наумчук, К. М., Тростенюк Т. М., Васильєва, Н. В., Alhogail, A., Kum ar, S., Biswas, B., Bhatia, M.S., Dora, M., Owusu Kwateng, K., Loock, M. Amanor, C., Kritzinger, E., Amankwa, E Tetteh, F.K., Pandey, S., Singh, R.K., G unasekaran, A., Kaushik, A. [1-11] та інші автори.

Мета та завдання статті. Метою наукової статті є проведення комплексного аналізу сучасних викликів та перспектив інформаційної безпеки у системі публічного управління. Основний акцент робиться на розкритті проблем, що виникають через зростання кількості та складності кіберзагроз, а також на розробці стратегій та заходів для забезпечення ефективного захисту конфіденційної інформації та надійності систем управління.

Завдання дослідження:

1. Аналіз сучасних трендів та тенденцій в кіберзахисті.

2. Визначення та розгляд основних проблем, з якими стикаються органи публічного управління у сфері інформаційної безпеки, зокрема, витоків конфіденційної інформації, кібершпигунства, та маніпуляцій громадською думкою через інтернет-платформи.

3. Вивчення сучасних стратегій та методів захисту.

4. Оцінка впливу кіберзагроз на соціальні та політичні процеси.

5. Розробка рекомендацій рівня інформаційної безпеки.

Виклад основного матеріалу. Аналіз сучасних трендів та тенденцій в кіберзахисті є надзвичайно актуальною задачею в умовах стрімкого технологічного розвитку та постійного зростання кількості кіберзагроз. Сучасні технологічні досягнення визначають нові вимоги до захисту інформації в системах публічного управління. Зростання використання штучного інтелекту (ШІ) в сфері кіберзахисту стає значущим трендом. Системи машинного навчання використовуються для виявлення аномального поведінки та швидкого реагування на потенційні загрози. Одним із технологічних трендів є використання блокчейн-технологій для забезпечення надійності та прозорості систем кіберзахисту. Розподілена структура блокчейну може ускладнити завдання хакерів і покращити цілісність систем.

Сучасні органи публічного управління стикаються зі значущими викликами у сфері інформаційної безпеки, що народжуються з розвитком технологій та інтернет-платформ. Однією з основних проблем є виток конфіденційної інформації, який може стати наслідком недостатнього контролю над доступом до даних або недоліків в системах безпеки. Кібершпигунство визначає іншу серйозну загрозу, що стає дедалі більш вдосконаленою та складною. Зокрема, іноземні агенти можуть використовувати технології для здійснення кібершпигунства, зокрема витягуючи конфіденційні дані або отримуючи доступ до критичних інформаційних ресурсів [1].

Використання шифрування в розробці нових форм кіберзагроз робить важчим виявлення та вивчення їхніх характеристик – табл. 1.

Глобалізація інформаційних систем створює виклик у вигляді потенційного впливу зовнішніх акторів на інформаційну безпеку країни, що вимагає розробки ефективних міжнародних стратегій безпеки.

Необхідність забезпечення безпеки великого обсягу даних та їхньої обробки у реальному часі ставить перед органами управління завдання ефективної кібербезпеки без втрати швидкості та продуктивності. Постійна еволюція кіберзагроз, така як розумні атаки, що адаптовуються до захисту, ускладнює прогнозування та виявлення нових форм кіберзлочинності [2].

Таблиця 1

Види кіберзагроз, їх характеристики та унікальність можливостей, що створюють небезпеку життєво важливим національним інтересам держави

Види кіберзагроз	Характеристики	Унікальність
Фішинг [2]	Спроби отримання конфіденційної інформації, представляючи себе як довірене джерело.	Фішинг є поширеним методом через соціальний інжиніринг та різноманітні підходи, що роблять його важко виявити.
Мальвара [3]	Вторгнення в систему за допомогою шкідливих програм для отримання контролю чи викрадення інформації.	Мальвара часто модифікується, використовує різні вектори поширення та може обходити антивірусні програми.
DDoS-атака [4]	Надмірне завантаження серверів або мережі, що призводить до відмови в обслуговуванні.	DDoS-атаки можуть бути масштабними та розподіленими, важко фільтровані та потребують надійних заходів захисту.
Зловмисне програмне забезпечення [5]	Використання шкідливого програмного коду для незаконного доступу до системи чи шифрування інформації.	Зловмисне програмне забезпечення постійно змінюється, шифрується та може використовувати низькорівневі техніки атак.
Соціальний Інжиніринг [6]	Використання маніпуляцій та обману для отримання конфіденційної інформації від користувачів.	Цей метод залежить від вміння зловмисника обманювати та використовувати психологічні та соціальні фактори.
Zero-Day Вразливість [7]	Використання вразливості в програмному забезпеченні, яку розробник ще не виправив.	Zero-Day атаки можуть бути надзвичайно швидкими та важко виявлятися, оскільки вони використовують нові, ще не відомі вразливості.
Витік Даних [8]	Неправомірне отримання та розголошення конфіденційної інформації про користувачів чи організації.	Витік даних часто викликає серйозні наслідки для репутації та може бути важко визначити через швидкий розповсюджений характер інформації.

Віртуалізація та хмарні технології роблять гнучкішими та доступними системи, але водночас створюють нові пункти вразливості, які потребують уваги та захисту. Брак стандартизації та загальноприйнятих норм кібербезпеки може призвести до невідповідностей у рівнях захисту та розробки стратегій в різних галузях публічного управління. Автоматизація та інтеграція інформаційних систем збільшують продуктивність, але одночасно вносять ризики в сферу кібербезпеки, особливо при недостатньому захисті перед атаками [3].

Сучасне дослідження в області інформаційної безпеки фокусується на вивченні та удосконаленні стратегій та методів захисту інформації в системах публічного управління. Однією з ключових складових цього дослідження є аналіз існуючих антивірусних програм, які спроектовані для виявлення та усунення шкідливих програм, що можуть загрожувати безпеці систем [4].

Захист від фішингу є іншою важливою стратегією, що привертає увагу науковців та спеціалістів з інформаційної безпеки. Дослідження зосереджуються на виявленні та запобіганні атакам, які використовують соціальний інжиніринг для отримання конфіденційної інформації від користувачів [4].

Криптографічні засоби та методи є невід'ємною частиною сучасної стратегії захисту інформації. Дослідження у цій області охоплюють розробку та аналіз алгоритмів шифрування, стійкість яких до атак забезпечує надійний захист конфіденційної інформації під час передачі та зберігання [5].

Методи виявлення вторгнень представляють собою ефективні інструменти для виявлення аномалій та ненормальної активності в системах публічного управління. Дослідження у цій галузі включають розробку алгоритмів та технологій, спрямованих на раннє виявлення та запобігання потенційним загрозам. Ефективність багаторівневих стратегій захисту, які включають у себе як апаратні, так і програмні засоби, привертає увагу дослідників [6].

Аналіз та розвиток сучасних технологій для забезпечення анонімності та захисту приватності в онлайн-середовищі є однією з ключових областей дослідження. Розробка інструментів та практик, що забезпечують анонімність користувачів, є важливою для запобігання неправомірному збору та використанню особистих даних. Удосконалення механізмів моніторингу та аналізу подій у реальному часі є важливим завданням. Впровадження систем, які забезпечують постійний моніторинг та реагування на потенційні загрози в реальному часі, є ефективним способом зменшення ризиків [7].

Розробка та впровадження механізмів автоматизованого реагування на кіберзагрози, включаючи розпізнавання та блокування шкідливих програм, є активною областю дослідження. Авто-

матичні системи можуть прискорити виявлення та відповідь на загрози [8].

Інтеграція технологій штучного інтелекту (ШІ) в системи кібербезпеки забезпечує новий рівень ефективності. Аналіз поведінки та використання ШІ для прогнозування та запобігання атак дозволяє створити більш адаптивні та інтелектуальні системи захисту [9].

Вивчення впливу кіберзагроз на соціальні та політичні процеси є актуальною галуззю досліджень, оскільки кібератаки можуть серйозно впливати на функціонування сучасних суспільств. Вказані аспекти стають предметом серйозних обговорень, оскільки виникнення кіберзагроз може порушити демократичні процеси та підірвати стабільність у державі. Кіберзагрози можуть впливати на політичні аспекти шляхом маніпулювання громадською думкою через соціальні мережі та медіа, що ставить під сумнів автентичність інформації та розмиває границі між правдивістю та дезінформацією [8].

Спроби кібершпигунства можуть мати серйозний вплив на національну безпеку та зовнішню політику держави, викриваючи конфіденційні дані та секрети. Виникнення кіберзагроз може призводити до зменшення довіри громадян до державних інститутів, оскільки вони відчувають загрозу для своєї приватності та безпеки [10].

Успішні кібератаки можуть викликати паніку та хаос у суспільстві, що негативно впливає на стабільність та ефективність держави.Підвищення кількості та різноманітності кіберзагроз свідчить про необхідність постійного аналізу та вдосконалення стратегій захисту.

Дослідження вказують на необхідність створення міжнародних стандартів та механізмів співпраці для протидії транснаціональним кіберзагрозам. Виникнення кіберзагроз може призвести до економічних втрат та порушення зв'язків з іноземними партнерами через витік конфіденційної інформації. Розвиток технологій штучного інтелекту та машинного навчання відкриває нові можливості для кіберзагроз та вимагає постійного адаптування захисних стратегій. Освітні ініціативи та підвищення інформаційної грамотності громадян є необхідними для зменшення вразливості суспільства перед кіберзагрозами. Важливо враховувати, що кіберзагрози можуть бути використані для реалізації політичних цілей, впливаючи на геополітичні відносини та міжнародну політику [11].

Отже, на основі аналізу інформаційної безпеки у системі публічного управління можна сформулювати конкретні рекомендації для захисту та збереження даних:

1. Підвищення свідомості та навчання персоналу. Запровадження обов'язкових навчальних курсів з інформаційної безпеки для всього персоналу систем публічного управління, що може включати регулярні тренінги, семінари та онлайн-курси.

2. Створення ефективної політики паролів. Визначення строгих вимог щодо паролів, включаючи їхню довжину, складність та періодичність зміни.

3. Аудит безпеки систем. Проведення регулярних аудитів та відстеження діяльності в мережі для виявлення можливих аномалій та несправностей. Визначення та усунення недоліків у системах.

4. Шифрування конфіденційної інформації. Впровадження шифрування для захисту конфіденційних даних в період їх передачі та зберігання. Це може включати як шифрування файлів, так і шифрування з'єднань мережі.

5. Захист від малозначущих пристроїв. Визначення та обмеження доступу непрофільних пристроїв до мережі, щоб запобігти можливим загрозам від підключених до мережі пристроїв, які можуть бути вразливими.

6. Використання сучасних антивірусних рішень. Активне використання найновіших антивірусних програм захисту для виявлення та блокування шкідливих програм.

7. Створення регулярних резервних копій. Регулярне створення та зберігання резервних копій важливої інформації, що дозволить відновити дані в разі втрати або атаки.

8. Моніторинг та виявлення загроз. Встановлення систем моніторингу та виявлення загроз для оперативного реагування на потенційні атаки.

Висновки та пропозиції. У світлі проведеного аналізу сучасних трендів в кіберзахисті в системі публічного управління, можна визначити, що різновидність кіберзагроз стрімко зростає. Технологічні та соціальні тенденції визначають нові виклики, зокрема, розширення атак на основі штучного інтелекту та зростання кількості кіберзагроз, спрямованих на маніпулювання громадською думкою. Нові форми атак вимагають постійного вдосконалення заходів кіберзахисту та стратегій відповіді на ці загрози. Дослідження викликів у сфері інформаційної безпеки показало, що органи публічного управління стикаються зі значущими проблемами. Витоки конфіденційної інформації, кібершпигунство та маніпуляції громадською думкою стають системними проблемами, що потребують комплексного підходу до вирішення. Забезпечення надійності інформаційної безпеки вимагає посилення заходів у сферах превентивних заходів, детектування та

реагування на інциденти. Аналіз існуючих стратегій та методів захисту інформації в системах публічного управління підкреслив важливість комплексного підходу до кібербезпеки. Від антивірусних програм до криптографічних засобів та методів виявлення вторгнень, кожен інструмент має своє місце у загальній стратегії. Наголошено на необхідності постійного оновлення та вдосконалення заходів забезпечення безпеки для ефективного протидії сучасним кіберзагрозам. Дослідження впливу кіберзагроз на соціальні та політичні аспекти державного управління вказує на серйозні загрози для демократичних процесів та стабільності суспільства. Кібератаки можуть стати інструментом маніпулювання громадською думкою та навіть загрожувати фундаментальним принципам демократії. Рекомендується негайне впровадження заходів для запобігання та ефективної реакції на ці загрози. На основі отриманих результатів дослідження наведено конкретні рекомендації для підвищення рівня інформаційної безпеки в системах публічного управління. Важливими стратегічними напрямками є підвищення кваліфікації персоналу через навчання та тренінги, впровадження інноваційних технологічних рішень та посилення співпраці між різними секторами для ефективного реагування на сучасні виклики і загрози кіберпростору.

REFERENCES:

1. Usyk, S. (2021). DOSLIDZhENNIA PRAVOVOHO MEKHANIZMU ZABEZPEChENNIA INFORMATSIINOI BEZPEKY V UMOVAKH NADZVYCHAINYKH SYTUATSII [STUDY OF THE LEGAL MECHANISM FOR PROVIDING SECURITY INFORMATION IN EMERGENCIES]. Naukovyi visnyk: *Derzhavne upravlinnia / Scientific Bulletin: State Administration*, (4(6), 266–280. https://doi.org/10.32689/2618-0065-2020-4(6)-266-280 [in Ukrainian]

2. (2024), "Exploring the critical success factors of information security management: a mixed-method approach", *Information and Computer Security,* Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/ICS-03-2023-0034 [in English]

3. Citation Tuna, A.A. and Türkmendağ, Z. (2022), "Cyber Business Management", Özsungur, F. (Ed.) *Conflict Management in Digital Business, Emerald Publishing Limited, Leeds,* pp. 281-301. https://doi.org/10.1108/978-1-80262-773-220221026 [in English]

4. Sun, Y., Zhang, Y.-F., Wang, Y. and Zhang, S. (2023), "Cooperative governance mechanisms for personal information security: an evolutionary game approach", *Kybernetes,* Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/K-04-2023-0717 [in English]

5. 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]

6. Alhogail, A. (2021), "Enhancing information security best practices sharing in virtual knowledge communities", *VINE Journal of Information and Knowledge Management Systems*, Vol. 51 No. 4, pp. 550-572. https://doi.org/10.1108/VJIKMS-01-2020-0009 [in English]

7. Kumar, S., Biswas, B., Bhatia, M.S. and Dora, M. (2021), "Antecedents for enhanced level of cyber-security in organisations", *Journal of Enterprise Information Management,* Vol. 34 No. 6, pp. 1597-1629. https://doi.org/10.1108/JEIM-06-2020-0240 [in English]

8. Owusu Kwateng, K., Amanor, C. and Tetteh, F.K. (2022), "Enterprise risk management and information technology security in the financial sector", *Information and Computer Security,* Vol. 30 No. 3, pp. 422-451. https://doi.org/10.1108/ICS-11-2020-0185 [in English]

9. Pandey, S., Singh, R.K., Gunasekaran, A. and Kaushik, A. (2020), "Cyber security risks in globalized supply chains: conceptual framework", *Journal of Global Operations and Strategic Sourcing,* Vol. 13 No. 1, pp. 103-128. https://doi.org/10.1108/JGOSS-05-2019-0042 [in English]

10. Vasylieva, N. V. (2022). PROPAHANDA YAK SKLADOVA INFORMATSIINO-KOMUNIKATYVNOI POLITYKY I ZAHROZA NATSIONALNII BEZPETSI [PROPAGANDA AS A COMPONENT OF INFORMATION AND COMMUNICATION POLICY AND A THREAT TO NATIONAL SECURITY]. *Tavriiskyi naukovyi visnyk. Seriia: Publichne upravlinnia ta administruvannia / Taurian Scientific Herald. Series: Public management and administration*, (2), 34-41. https://doi.org/10.32851/tnv-pub.2022.2.5 [in Ukrainian]

11. Amankwa, E., Loock, M. and Kritzinger, E. (2022), "The determinants of an information security policy compliance culture in organisations: the combined effects of organisational and behavioural factors", *Information and Computer Security,* Vol. 30 No. 4, pp. 583-614. https://doi.org/10.1108/ICS-10-2021-0169 [in English]