DOI 10.52363/2414-5866-2025-1-16
УДК 355/359.07; 342.08

Філонов М.В., *аспірант Класичного приватного університету, м. Запоріжжя, ORCID: 0009-0001-3958-5822*

Filonov M., *Postgraduate student of the Classic Private University, Zaporizhzhia*

ПЕРСПЕКТИВИ РОЗВИТКУ МЕХАНІЗМІВ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РЕГІОНАЛЬНОМУ РІВНІ

PROSPECTS FOR THE DEVELOPMENT OF PUBLIC ADMINISTRATION MECHANISMS IN THE FIELD OF INFORMATION SECURITY AT THE REGIONAL LEVEL

Визначено перспективи розвитку механізмів публічного управління у сфері інформаційної безпеки на регіональному рівні. Серед них виокремлено такі: підвищення цифрової й інформаційної грамотності населення; аудит безпеки систем на регулярній основі; шифрування конфіденційної інформації; розробка та впровадження регіональних стратегій інформаційної безпеки, які будуть ураховувати вимоги часу та суспільства та ін.

Ключові слова: *публічне управління, сфера інформаційної безпеки, стратегія інформаційної безпеки, органи державної влади, регіони.*

Prospects for the development of public administration mechanisms in the field of information security at the regional level have been identified. Among them, the following are highlighted: increasing the digital and information literacy of the population; regular system security audits; encryption of confidential information; development and implementation of regional information security strategies that will take into account the requirements of time and society, etc.

Keywords: *public administration, information security sphere, information security strategy, state authorities, regions.*

Постановка проблеми. Інформаційна безпека у сфері державного управління набуває в сучасному світі критичного значення, що пов'язано з

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

багатьма викликами та можливостями. Сучасні тенденції очевидно показують, що кібератаки стають дедалі частішими, а їх складність та різноманітність створюють серйозні труднощі для забезпечення ефективного функціонування управлінських систем. Згідно з останньою статистикою, спостерігається значне збільшення кількості кібератак на урядові структури. За останні роки частішають інциденти, пов'язані з незаконним доступом до конфіденційних даних, витоками інформації та порушенням роботи критичних систем управління. Наприклад, державний центр кіберзахисту повідомляє, що лише за минулий рік атаки на державні управлінські установи зросли на 30%. Зважаючи на ці виклики та тенденції, науковці та влада повинні об'єднати зусилля для розробки та впровадження нових стратегій і рішень, які зміцнять інформаційну безпеку в системах державного управління.

Аналіз останніх досліджень і публікацій. Розгляду особливостей формування та реалізації державної політики у сфері інформаційної безпеки присвячені публікації таких науковців, як Я. Базилюк, А. Гриценко, М. Денисенко, С. Домбровська, А. Карсруд, Р. Клют, П. Колісніченко, С. Лекар, В. Орлик, Г. Почепцов та інших [1; 3].

Постановка завдання. Метою статті є визначити перспективи розвитку механізмів публічного управління у сфері інформаційної безпеки на регіональному рівні.

Виклад основного матеріалу. Аналіз сучасних трендів і тенденцій у сфері кіберзахисту є вкрай важливим завданням в умовах швидкого технологічного розвитку та постійного зростання кількості кіберзагроз. Нинішні технологічні досягнення встановлюють нові вимоги до захисту інформації в системах державного управління. Зростаюче використання штучного інтелекту у кіберзахисті стає помітним трендом. Системи машинного навчання допомагають виявляти аномальну поведінку та швидко реагувати на потенційні загрози. Одним з технологічних трендів є впровадження блокчейн-технологій для підвищення надійності та прозорості систем кіберзахисту. Розподілена структура блокчейну ускладнює завдання для хакерів і покращує цілісність систем. Сучасні органи державного управління стикаються зі значними викликами у сфері інформаційної безпеки, які виникають через розвиток технологій та інтернет-платформ. Однією з головних проблем є витік конфіденційної інформації, що може статися через недостатній контроль доступу до даних або слабкі місця в системах безпеки. Кібершпигунство є іншою серйозною загрозою, яка стає дедалі складнішою. Зокрема, іноземні агенти можуть використовувати технології для кібершпигунства, витягуючи конфіденційні дані або отримуючи доступ до критично важливих інформаційних ресурсів [1].

Глобалізація інформаційних систем створює ризик впливу зовнішніх акторів на інформаційну безпеку країни, що вимагає розробки

ефективних міжнародних стратегій безпеки. Забезпечення безпеки великої кількості даних та їх обробка в реальному часі ставить перед органами управління завдання ефективної кібербезпеки без втрати швидкості та продуктивності. Постійна еволюція кіберзагроз, таких як адаптивні атаки, ускладнює прогнозування і виявлення нових форм кіберзлочинів [2].

Віртуалізація і хмарні технології роблять системи більш гнучкими та доступними, проте створюють нові уразливості, що потребують уваги і захисту. Відсутність стандартизації і загальноприйнятих кібербезпекових норм може призвести до різних рівнів захисту та розробки стратегій у сфері публічного управління. Автоматизація й інтеграція інформаційних систем підвищують продуктивність, але водночас додають ризики в сферу кібербезпеки, особливо при недостатньому захисті від атак. Модерні дослідження в області інформаційної безпеки зосереджуються на вдосконаленні стратегій і методів захисту даних у системах публічного управління [3].

Одним з ключових аспектів цього є аналіз антишкідливих програм, призначених для виявлення і нейтралізації загрозливого програмного забезпечення. Захист від фішинг-атак також важлива сфера уваги дослідників і спеціалістів, вони працюють над розпізнаванням та запобіганням атакам соціального інжинірингу, спрямованим на отримання конфіденційної інформації від користувачів. Криптографічні засоби та методи є невід'ємною складовою сучасних стратегій захисту даних [4].

Дослідження в цій області охоплюють розробку і аналіз алгоритмів шифрування, чиї стійкість до атак забезпечує надійний захист конфіденційних даних при передачі і зберіганні. Методи виявлення вторгнень ефективно вирізняють аномалії та ненормальну активність в системах публічного управління. Дослідження тут включають створення алгоритмів і технологій, спрямованих на раннє виявлення та запобігання потенційним загрозам. Ефективність багаторівневих стратегій захисту, що об'єднують як апаратні, так і програмні засоби, становить значний інтерес для дослідників [5; 6].

Аналіз сучасних технологій для забезпечення анонімності та захисту приватності в онлайн-середовищі є однією з ключових сфер дослідження. Розробка інструментів та практик, що дозволяють користувачам зберігати анонімність, має важливе значення для запобігання неправомірному збору та використанню особистих даних. Удосконалення механізмів моніторингу та аналізу подій у реальному часі є необхідним завданням [7].

Впровадження систем для постійного моніторингу та швидкого реагування на потенційні загрози ефективно знижує ризики. На основі аналізу інформаційної безпеки у системі публічного управління можна

визначити конкретні рекомендації для захисту та збереження даних:

1. Підвищення свідомості та навчання персоналу. Запровадження обов'язкових освітніх програм з інформаційної безпеки для всього персоналу, включаючи регулярні тренінги, семінари та онлайн-курси.

2. Створення ефективної політики паролів. Встановлення строгих вимог до паролів щодо довжини, складності та регулярності їх зміни.

3. Аудит безпеки систем. Проведення регулярних перевірок та моніторингу мережевої діяльності для виявлення потенційних аномалій та несправностей, а також усунення недоліків в системах.

4. Шифрування конфіденційної інформації. Використання шифрування для захисту даних під час їх передачі та зберігання, включаючи файли та мережеві з'єднання.

5. Захист від некоректних пристроїв. Ідентифікація та обмеження доступу несумісних пристроїв до мережі, щоб запобігти можливим загрозам від підключених уразливих пристроїв.

6. Використання сучасних антивірусних рішень. Застосування найновіших антивірусних програм для виявлення та блокування шкідливого програмного забезпечення.

7. Створення регулярних резервних копій. Регулярне створення і збереження резервних копій, що дозволить відновити дані у випадку їх втрати або атаки.

8. Моніторинг та виявлення загроз. Інсталяція систем для моніторингу та виявлення загроз, що забезпечать оперативну реакцію на потенційні атаки.

Висновки. У світлі аналізу сучасних тенденцій у сфері кіберзахисту в системі публічного управління стає очевидним, що кількість кіберзагроз збільшується з великою швидкістю. Технологічні та соціальні зміни відкривають нові виклики, такі як атаки, що використовують штучний інтелект, і зростання нападів з метою маніпуляції громадською думкою. Ці нові форми загроз вимагають постійного покращення заходів безпеки та стратегій реагування. Дослідження у сфері інформаційної безпеки виявило, що органи публічного управління стикаються з серйозними проблемами. Витік конфіденційної інформації, кібершпигунство та маніпуляція громадською думкою перетворилися на системні загрози, що вимагають комплексного підходу до вирішення. Надійність інформаційної безпеки потребує посилення заходів у сферах превентивних дій, виявлення та швидкого реагування на інциденти. Аналіз наявних стратегій і методів захисту інформації підкреслив важливість цілісного підходу до кібербезпеки. Від антивірусних програм до криптографічних засобів і методів виявлення вторгнень — кожен інструмент грає важливу роль у загальній стратегії. Є необхідність постійного оновлення й удосконалення заходів для ефективної протидії сучасним кіберзагрозам. Дослідження

впливу кіберзагроз на соціальні та політичні аспекти державного управління вказує на значну небезпеку для демократичних процесів і стабільності суспільства. Кібератаки можуть стати засобом маніпуляції громадською думкою і навіть загрожувати основам демократії. Необхідно терміново впровадити заходи для запобігання та ефективної реакції на ці ризики. На основі отриманих даних розроблено конкретні рекомендації для покращення інформаційної безпеки в системах публічного управління. Серед важливих стратегічних напрямків — підвищення кваліфікації співробітників через навчання та тренінги, впровадження інноваційних технологічних рішень і зміцнення співробітництва між різними секторами для оперативної відповіді на сучасні виклики й загрози кіберпростору.

Список використаних джерел:

1. Домбровська С.М., Помаза-Пономаренко А.Л., Крюков О.І., Порока С.Г. Інформаційні загрози та комунікативна інфраструктура в державному секторі : монографія. 2024. Харків: НУЦЗУ. 244 с. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.
2. "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.
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.
4. Sun, Y., Zhang, Y.-F., W ang, 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.
5. 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/
6. 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.
7. Owusu Kwateng, K., Amanor , C. and T etteh, 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.

References:

1. Dombrovska S.M., Pomaza-Ponomarenko A.L., Kryukov O.I., Poroka S.G. Information threats and communication infrastructure in the government sector: monograph. 2024. Kharkiv: NUTSZU. 244 p. URL: http://repositsc.nuczu.edu.ua/handle/123456789/19990.

2. "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.

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.

4. Sun, Y., Zhang, Y.-F., W ang, 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.

5. 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/

6. 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.

7. Owusu Kwateng, K., Amanor , C. and T etteh, 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.

дата надходження статті: 16.04.2025
дата прийняття статті: 20.05.2025
дата публікації: 25.06.2025