Функціонування і розвиток механізмів державного управління

УДК 351.72:004.056.5

Нагорняк Михайло Миколайович
доктор політичних наук, професор,
професор кафедри управління та бізнес-адміністрування
Прикарпатський національний університет імені Василя Стефаника
Nahorniak Mykhaylo
Doctor of Political Sciences, Professor,
Professor of the Department of Management and Business Administration
Vasyl Stefanyk Prykarpattia National University
ORCID: 0000-0001-8947-3450

СТРАТЕГІЇ ПУБЛІЧНОГО УПРАВЛІННЯ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У СФЕРІ НАДАННЯ ЕЛЕКТРОННИХ ПОСЛУГ: ПРАКТИКИ ТА РЕКОМЕНДАЦІЇ
STRATEGIES OF PUBLIC MANAGEMENT TO COMBAT CYBER THREATS IN THE FIELD OF ELECTRONIC SERVICES: PRACTICES AND RECOMMENDATIONS

Анотація. *У сучасному світі, де використання електронних технологій стає все більш широким, а доступ до публічних послуг через Інтернет стає стандартом, питання кібербезпеки набуває все більшої актуальності. Кіберзагрози, такі як кібератаки, витік конфіденційної інформації та кібершпигунство, стають серйозними викликами для публічного управління. Особливо це стосується сфери надання електронних послуг, де швидкість розвитку технологій породжує нові загрози безпеці. Зростання кількості та складності кіберзагроз ставить під сумнів цю мету. Стратегії публічного управління є ключовим інструментом для забезпечення ефективного функціонування суспільства*

в умовах високих технологічних викликів. Зростання кількості кіберзагроз у сфері надання електронних послуг надає актуальності розробці та впровадженню стратегій, спрямованих на їх протидію. Відповідно, необхідно розробити та впровадити стратегії публічного управління, спрямовані на протидію кіберзагрозам у сфері надання електронних послуг, з урахуванням сучасних трендів та тенденцій. Останнім часом спостерігається зростання як кількості кібератак, так і їхньої складності. Кіберзлочинці стають все винахідливішими у використанні нових методів атак та обходженні захисту, що призводить до збільшення вимог до захисту конфіденційної інформації та підвищення важливості стандартів безпеки. Гіпотези дослідження передбачають, що розробка та впровадження комплексних стратегій публічного управління, які включатимуть технологічні, організаційні та освітні заходи, сприятиме ефективнішій боротьбі з кіберзагрозами. Залучення широких мас населення до культури кібербезпеки також може сприяти зменшенню ризиків кібератак та витоків даних. Збільшення кількості інцидентів кібербезпеки в секторі публічного управління, яке свідчить про необхідність активного впровадження заходів протидії кіберзагрозам для забезпечення безпеки та надійності електронних послуг для громадян.

Ключові слова: *публічне управління, механізми публічного управління, інформаційна безпека, електронні послуги, публічне управління інформаційною безпекою, публічне управління наданням електронних послуг.*

Summary. *In today's world, where the use of electronic technologies is becoming more and more widespread, and access to public services over the Internet becomes the standard, the issue of cybersecurity is gaining increasing relevance. Cyber threats, such as cyber-attacks, confidential information leaks and cyber espionage, are becoming serious challenges for public*

administration. This is especially true in the field of electronic services, where the speed of technology development creates new security threats. The increasing number and complexity of cyber threats calls this goal into question. Public administration strategies are a key tool for ensuring the effective functioning of society in conditions of high technological challenges. The increase in the number of cyber threats in the field of electronic services provides relevance to the development and implementation of strategies aimed at their counteraction. Accordingly, it is necessary to develop and implement public administration strategies aimed at counteracting cyber threats in the field of electronic services, taking into account current trends and trends. Recently there is an increase in both the number of cyber-attacks and their complexity. Cybercriminals are becoming increasingly ingenious in using new methods of attack and circumvention, leading to increased demands on confidential information protection and increased importance of security standards. The research hypotheses suggest that the development and implementation of integrated public administration strategies, which will include technological, organizational and educational measures, will contribute to a more effective fight against cyber threats. Involving the masses of the population in the culture of cybersecurity can also help reduce the risk of cyber-attacks and data leaks. Increase in the number of cyber security incidents in the public administration sector, which indicates the need for active implementation of measures to counter cyber threats to ensure the security and reliability of electronic services for citizens.

Key words: *public management, mechanisms of public management, information security, electronic services, public management of information security, public management of the provision of electronic services.*

Постановка проблеми. У світі, де електронні технології набувають все більшого значення, а доступ до електронних послуг стає необхідністю,

кіберзагрози в сфері надання таких послуг стають все більш серйозною проблемою. За даними Міжнародного центру кібербезпеки, у 2023 році вже зареєстровано понад 500 тисяч інцидентів кібербезпеки в сфері надання електронних послуг, що на 15% перевищує показники попереднього року та встановлено, що кіберзагрозами стали об'єкти, які раніше вважалися менш вразливими, такі як місцеві державні установи та малий бізнес. Систематичний аналіз і вдосконалення законодавства щодо кібербезпеки сприятиме створенню стійкого середовища для боротьби з кіберзагрозами.

Аналіз останніх досліджень і публікацій. Питання публічного управління, зокрема питання протидії кіберзагрозам у сфері надання електронних послуг досліджуються як вітчизняними, так і зарубіжними науковцями, серед яких: Сиротін В. [1], Приймаченко Д., Мінка Т. [2], Куспляк Г., Куспляк І., Серенок А. [3], Гончарук Н. [4] та ін. Деякі дискусійні питання щодо публічного управління в контексті протидії кіберзагрозам у сфері надання електронних послуг не були досліджені у повній мірі вітчизняними науковцями та потребують ретельного опрацювання.

Мета статті. Метою дослідження є розгляд сучасних стратегій публічного управління для протидії кіберзагрозам у сфері надання електронних послуг, а також надати рекомендації для підвищення ефективності заходів з кібербезпеки в сфері публічного управління.

Виклад основного матеріалу. Сучасні тенденції у сфері кібербезпеки мають значний вплив на надання електронних послуг публічними органами. Деякі з найбільш значущих тенденцій включають:

- Зростання кількості кібератак.
- Розширення атакованих об'єктів.
- Використання нових технологій для атак.
- Фокус на захист особистих даних.

– Зростання обізнаності та освіти в галузі кібербезпеки [5].

Тенденції покладають великий тиск на публічні органи, щоб постійно вдосконалювати свої стратегії кібербезпеки та гарантувати надійне та безпечне надання електронних послуг для своїх громадян.

Різні країни використовують різноманітні стратегії публічного управління для протидії кіберзагрозам, враховуючи їхні унікальні потреби, рівень розвитку кіберінфраструктури та юридичний контекст (табл.1).

Таблиця 1

Стратегії публічного управління для протидії кіберзагрозам [6]

Стратегія	Опис
Створення національних центрів кібербезпеки	Багато країн розвивають національні центри кібербезпеки, які координують дії з протидії кіберзагрозам на національному рівні. Центри забезпечують обмін інформацією, аналізують загрози та надають рекомендації з кібербезпеці.
Заохочення публічно-приватного партнерства	Деякі країни активно залучають приватний сектор до співпраці з публічними органами у сфері кібербезпеки, що може включати обмін інформацією, спільні навчальні програми та інші форми співпраці.
Створення регуляторних рамок	Деякі країни впроваджують строгі регуляторні вимоги щодо кібербезпеки для публічних органів та приватних компаній, що надають послуги електронного управління та рамки встановлюють стандарти безпеки та вимоги щодо звітності та відповідальності.
Розвиток та впровадження національних стратегій кібербезпеки	Багато країн розробляють та реалізують національні стратегії кібербезпеки, які визначають пріоритети, завдання та заходи з протидії кіберзагрозам на національному рівні.
Підвищення освіти та навчання з кібербезпеки	Багато країн розвивають програми підвищення освіти та навчання з кібербезпеки, які призначені для підготовки персоналу в публічному секторі та в інших галузях національної економіки.

Розглянуті стратегії можуть варіюватися в залежності від конкретних потреб та контексту кожної країни, але спільна мета полягає у забезпеченні безпеки та стабільності в сфері електронних послуг. Найефективніші практики та інноваційні підходи до захисту електронних послуг від кібератак постійно розвиваються, оскільки кіберзлочинці постійно вдосконалюють свої методи (рис. 1).

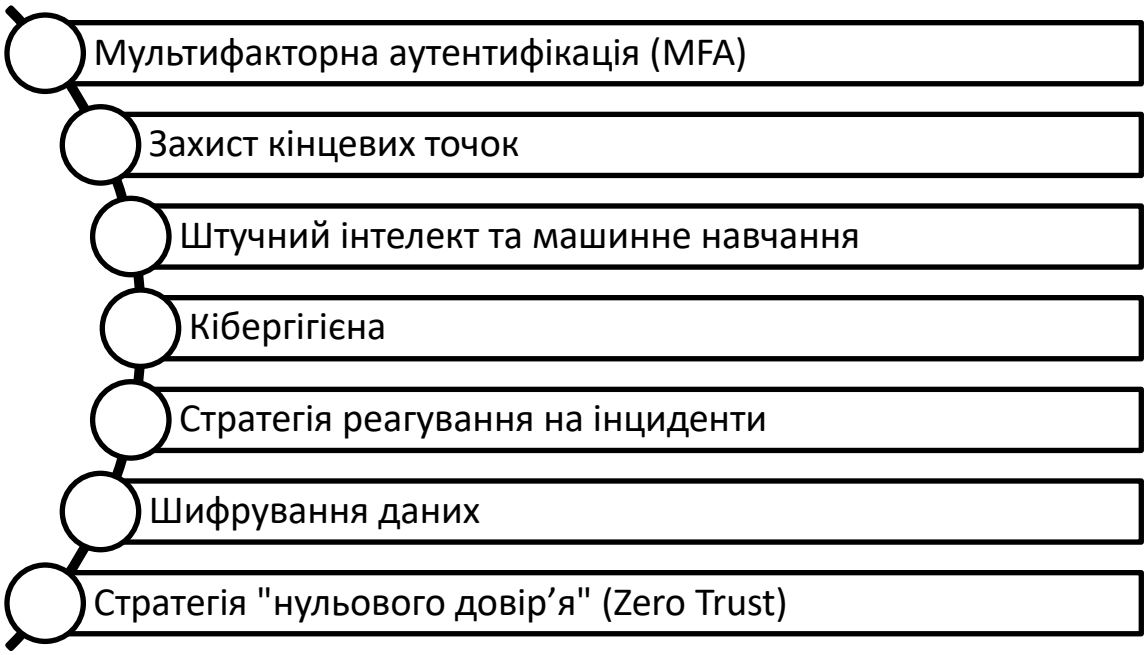

Рис. 1. Інноваційні підходи до захисту електронних послуг від кібератак

Джерело: [7]

Розглянемо детальніше кожен із інноваційних підходів до захисту електронних послуг від кібератак:

– Мультифакторна аутентифікація (MFA): використання не тільки пароля, але й додаткового механізму, такого як код підтвердження, відбиток пальця або мережевий ключ, для входу в систему, що ускладнює процес вторгнення для зловмисників.

– Захист кінцевих точок: розробка та впровадження захисних програм та механізмів на кінцевих точках, таких як антивірусне програмне забезпечення, захист від фішингу та контроль за дотриманням політик безпеки.

– Стратегія "нульового довір'я" (Zero Trust): підхід передбачає, що ніякий користувач або пристрій не повинен автоматично довірятися всередині мережі. Кожен запит на доступ до ресурсів мережі перевіряється та автентифікується перед наданням доступу.

– ШІ: використання алгоритмів штучного інтелекту та машинного навчання для виявлення аномальних зразків та підозрілих активностей в реальному часі, що дозволяє оперативно реагувати на потенційні загрози.

– Шифрування даних: використання шифрування для захисту конфіденційної інформації під час передачі та зберігання на серверах, що допомагає запобігти доступу до даних навіть у випадку їх несанкціонованого отримання.

– Кібергігієна: вдосконалення культури кібербезпеки серед персоналу, включаючи навчання з обізнаності щодо кібербезпеки, проведення регулярних тренінгів та стимулювання відповідальності за забезпечення безпеки в межах організації [8].

Розробка та впровадження комплексних стратегій публічного управління для забезпечення кібербезпеки в сфері електронних послуг вимагає уваги до різних ключових аспектів [9]. Перший крок у розробці стратегії - це аналіз потенційних загроз і ризиків для систем електронних послуг, що включає оцінку потенційних атак, ідентифікацію слабких місць у системах, визначення вразливостей та оцінку можливих наслідків інцидентів. На основі аналізу ризиків формулюються стратегічні цілі, які мають бути досягнуті для забезпечення кібербезпеки в електронних послугах та можуть включати покращення захисту інфраструктури, забезпечення конфіденційності та цілісності даних, підвищення свідомості про кібербезпеку серед персоналу та громадян тощо. На основі визначених цілей формулюється стратегія та політика кібербезпеки, яка визначає основні принципи, підходи та заходи, необхідні для досягнення цих цілей та повинна враховувати специфічні потреби та характеристики сектору електронних послуг. Забезпечення достатніх ресурсів, включаючи фінансові, технічні та людські ресурси, для впровадження стратегій кібербезпеки, що може включати виділення бюджету на кібербезпеку,

закупівлю необхідного обладнання та програмного забезпечення, навчання персоналу та залучення експертів [10].

Важливим аспектом є залучення всіх зацікавлених сторін, включаючи урядові органи, приватний сектор, академічні установи та громадські організації, до процесу розробки та впровадження стратегій кібербезпеки. Кіберзагрози постійно еволюціонують, тому важливо постійно оновлювати та адаптувати стратегії кібербезпеки для відповіді на нові виклики [11].

Дані аспекти є ключовими у розробці та впровадженні комплексних стратегій публічного управління для забезпечення кібербезпеки в сфері електронних послуг. Однак важливо пам'ятати, що кожна країна має свої унікальні характеристики та виклики, тому стратегії кібербезпеки повинні бути адаптовані до конкретного контексту кожної країни.

Висновки. Стратегії публічного управління для протидії кіберзагрозам у сфері надання електронних послуг є критично важливими для забезпечення безпеки та надійності цих послуг. Наукові дослідження, практичний досвід та рекомендації експертів дозволяють сформулювати ефективні стратегії, які відповідають викликам сучасного цифрового середовища. а основі аналізу загроз і ризиків необхідно розробляти комплексні стратегії публічного управління, які включають в себе широкий спектр заходів для ефективного захисту електронних послуг. Визначено, що кіберзагрози постійно змінюються, тому важливо підтримувати постійне вдосконалення стратегій та заходів кібербезпеки для ефективного протидії сучасним та майбутнім загрозам. В цілому, ефективні стратегії публічного управління в області кібербезпеки вимагають комплексного підходу, активного співробітництва та вдосконалення для забезпечення безпеки в сфері електронних послуг.

Література

1. Сиротін В. Цифрові тренди у сфері публічного управління. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2023. doi: 10.54929/2786-5746-2023-10-02-05.
2. Приймаченко Д., Мінка Т. Особливості оскарження органів публічної адміністрації щодо надання електронних послуг у сфері міграції та громадянства. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування.* 2022. doi: 10.54929/2786-5746-2022-6-01-14.
3. Куспляк Г., Куспляк І., Серенок А. Напрями вдосконалення надання адміністративних та публічних електронних послуг в умовах воєнного стану. *Теоретичні та прикладні питання державотворення.* 2023. С. 103-114. doi: 10.35432/tisb302023295150.
4. Goncharuk N., Pyrohova Yu., Suray I., Prokopenko L., Prudius L. Reformation Public Administration in Ukraine in the Context of European Integration: Current State, Problems and Priorities. *Economic Affairs.* 2023. Vol. 68, No. 03. doi: 10.46852/0424-2513.3.2023.27.
5. Ushakova E., Vinogradova T. Innovative Tools for Increasing the Openness and Transparency of Public-Private Partnership Projects. Economics and Management. 2021. № 27. P. 361-367. doi: https://doi.org/10.35854/1998-1627-2021-5-361-367.
6. Pysmenna M. Openness and transparency of public procurement: perspectives of legislative provisions. *Scientific Bulletin of Flight Academy. Section: Economics, Management and Law.* 2022. № 7. P. 123-128. doi: https://doi.org/10.33251/2707-8620-2022-7-123-128.
7. Korzh I. The principles of transparency and openness of the electronic parliament in the conditions of decentralization of the state power of Ukraine. *Information and law.* 2016. № 2(17). P. 32-42. doi: https://doi.org/10.37750/2616-6798.2016.2(17).272834.

8. Polley R., Clifton M.-J. The Principles of Transparency and Openness, and Access to Documents. *The Handbook of EEA Law.* 2016. P. 625–656. doi: https://doi.org/10.1007/978-3-319-24343-6_29.
9. Sydorovych R. The aspect of balance in the implementation of the principle of openness and transparency of the civil service institute: the issue of "Cyber sovereignity". *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences.* 2023. № 10. P. 28-33. doi: https://doi.org/10.23939/law2023.39.028.
10. Petlenko Yu., Drozd N., Morhun D. Openness and transparency of the budget process in Ukraine. *Scientific Bulletin of Flight Academy. Section: Economics, Management and Law.* 2021. № 5. P. 83-91. doi: https://doi.org/10.33251/2707-8620-2021-5-83-91.
11. Zubenko H. Principles of transparency, openness and publicity in the activities of non-governmental organizations. *The Journal of V N Karazin Kharkiv National University Series Law.* 2022. P. 56-61. Doi: https://doi.org/10.26565/2075-1834-2022-34-06.

References

1. Syrotin, V. (2023). Tsyfrovi trendy u sferi publichnoho upravlinnya [Digital trends in the field of public administration]. *Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya*. doi: 10.54929/2786-5746-2023-10-02-05 [in Ukrainian].
2. Pryymachenko, D., & Minka, T. (2022). Osoblyvosti oskarzhennya orhaniv publichnoyi administratsiyi shchodo nadannya elektronnykh posluh u sferi mihratsiyi ta hromadyanstva [Peculiarities of appealing to public administration bodies regarding the provision of electronic services in the field of migration and citizenship]. *Problemy suchasnykh transformatsiy. Seriya: pravo, publichne upravlinnya ta administruvannya*. doi: 10.54929/2786-5746-2022-6-01-14 [in Ukrainian].

3. Kusplyak H., Kusplyak, I., & Serenok, A. (2023). Napryamy vdoskonalennya nadannya administratyvnykh ta publichnykh elektronnykh posluh v umovakh voyennoho stanu [Directions for improving the provision of administrative and public electronic services under martial law]. *Teoretychni ta prykladni pytannya derzhavotvorennya*, 103-114. doi: 10.35432/tisb302023295150 [in Ukrainian].
4. Goncharuk, N. (2023). Reformation Public Administration in Ukraine in the Context of European Integration: Current State, Problems and Priorities. *Economic Affairs, 68*. doi: 10.46852/0424-2513.3.2023.27.
5. Ushakova, E., & Vinogradova, T. (2021). Innovative Tools for Increasing the Openness and Transparency of Public-Private Partnership Projects. *Economics and Management, 27,* 361-367. doi: https://doi.org/10.35854/1998-1627-2021-5-361-367.
6. Pysmenna, M. (2022). Openness and transparency of public procurement: perspectives of legislative provisions. *Scientific Bulletin of Flight Academy. Section: Economics, Management and Law, 7,* 123-128. doi: https://doi.org/10.33251/2707-8620-2022-7-123-128.
7. Korzh, I. (2016). The principles of transparency and openness of the electronic parliament in the conditions of decentralization of the state power of Ukraine. *Information and law, 2*(17), 32-42. doi: https://doi.org/10.37750/2616-6798.2016.2(17).272834.
8. Polley, R., . Clifton, M.-J. (2016). The Principles of Transparency and Openness, and Access to Documents. *The Handbook of EEA Law,* 625–656. doi: https://doi.org/10.1007/978-3-319-24343-6_29.
9. Sydorovych, R. (2023). The aspect of balance in the implementation of the principle of openness and transparency of the civil service institute: the issue of "Cyber sovereignity". *Bulletin of Lviv Polytechnic National University. Series: Legal Sciences, 10*, 28-33. doi: https://doi.org/10.23939/law2023.39.028.

10. Petlenko, Yu., Drozd, N., & Morhun, D. (2021). Openness and transparency of the budget process in Ukraine. *Scientific Bulletin of Flight Academy. Section: Economics, Management and Law, 5,* 83-91. doi: https://doi.org/10.33251/2707-8620-2021-5-83-91.
11. Zubenko, H. (2022). Principles of transparency, openness, and publicity in the activities of non-governmental organizations. *The Journal of V. N. Karazin Kharkiv National University Series Law,* 56-61. doi: https://doi.org/10.26565/2075-1834-2022-34-06.