Олег БОГАЧ
аспірант за освітньо-науковою програмою
«Публічне управління та адміністрування», ЗУНУ
Науковий керівник – Руслан АВГУСТИН, д-р. екон. наук,
професор, виконуючий обов'язки завідувача кафедри
менеджменту, публічного управління та персоналу
Західноукраїнського національного університету

МЕТОДОЛОГІЯ УПРАВЛІННЯ РИЗИКАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

За сучасних умов всеохоплюючої цифрової трансформації, інформація стала одним із визначальних ресурсів функціонування держави, бізнесу, територіальних громад та суспільства загалом. Більшість управлінських, фінансових, комунікаційних і соціальних процесів здійснюються із використанням цифрових технологій, інформаційних систем та мережевої взаємодії. Відбуваються невідворотні процеси посилення цифрової залежності, що в свою чергу бурудбачає можливості виникнення більшої кількості ризиків, пов'язаних із втратою, викраденням, пошкодженням або блокуванням інформації. Відтак, інформаційна безпека перестала бути виключно технічним питанням і вона дедалі більше перетворюється на необхідний елемент стратегічного управління. Крім того, кібератаки, витоки персональних даних, фішингові схеми, поширення дезінформації, технічні збої або людські помилки здатні суттєво порушувати стабільність роботи організацій та органів влади. Особливо небезпечними такі ризики є в умовах війни, кризових ситуацій та активної цифровізації управлінських процесів [1].

У зв'язку з цим, головним завданням методології управління ризиками інформаційної безпеки має стати не лише реагування на вже існуючі загрози, а насамперед їх своєчасне виявлення, оцінювання, попередження та мінімізація можливих наслідків. Такий підхід має базуватися на розумінні того, що повністю усунути всі загрози практично неможливо, однак ними можна системно

управляти, зменшуючи рівень вразливості інформаційних систем та підвищуючи загальну стійкість організації.

Ризики інформаційної безпеки мають різну природу та джерела виникнення. Частина з них пов'язана з технічними проблемами, інші ж ризики виникають через організаційні недоліки, відсутність чітких правил роботи з інформацією, недостатній контроль доступу або помилки персоналу. Значну небезпеку також становить людський фактор, так як значна частина кіберінцидентів виникає саме через певні дії працівників, відкриття підозрілих повідомлень та нехтування базовими правилами цифрової безпеки [3].

Практика свідчить, що навіть найсучасніші технічні засоби захисту не можуть гарантувати належний рівень безпеки без ефективної організації процесів та відповідного рівня цифрової культури персоналу. Це підтверджує, що методологія управління ризиками повинна охоплювати не лише захист комп'ютерних систем, а й формування внутрішньої політики безпеки, розвиток систем моніторингу, підготовку персоналу, антикризові комунікації та постійне вдосконалення механізмів реагування на загрози [4].

Одним із ключових етапів управління ризиками інформаційної безпеки територіальної громади є ідентифікація ризиків. На цьому етапі органи місцевого самоврядування повинні визначити, які інформаційні ресурси та цифрові сервіси є найбільш важливими для стабільного функціонування громади та які загрози можуть впливати на їхню роботу. Йдеться про аналіз електронного документообігу, баз даних мешканців, систем надання адміністративних послуг, фінансових платформ, офіційних сайтів громади, каналів цифрової комунікації та іншої інформаційної інфраструктури. Важливим завданням є своєчасне виявлення слабких місць, які можуть бути використані для кібератак, витоку інформації або порушення роботи цифрових сервісів. Саме раннє виявлення вразливостей дозволяє громадам мінімізувати можливі втрати та уникнути масштабних кризових ситуацій.

На рівні оцінювання ризиків керівництво громади має визначити ймовірність виникнення конкретних загроз та можливі

наслідки їх реалізації. Оцінювання доцільно проводити з урахуванням рівня критичності ризику, масштабів потенційних втрат, впливу на стабільність роботи органу місцевого самоврядування та здатності забезпечити безперервне надання послуг населенню.

Після оцінювання ризиків доцільно визначити методи реагування на них та реалізувати належне організаційне забезпечення цих процесів. Органи місцевого самоврядування повинні мати чіткі правила роботи з інформацією, визначений розподіл відповідальності між працівниками, алгоритми реагування на кіберінциденти та механізми внутрішнього контролю. Іншими словами, інформаційна безпека не повинна залишатися виключно сферою діяльності ІТ-фахівців, так як значна частина ризиків виникає саме через управлінські помилки, недостатню координацію дій або недосконалі внутрішні процедури. В цьому контексті зазначимо, що важливим елементом методології управління ризиками є також кадрова складова. Значна частина інформаційних інцидентів у громадах виникає через недостатній рівень цифрової грамотності або нехтування базовими правилами кібергігієни. Це доводить, що органи місцевого самоврядування повинні постійно інвестувати в навчання працівників, розвиток навичок безпечної роботи з інформацією, формування культури цифрової безпеки та підготовку персоналу до дій у кризових ситуаціях [2].

Невід'ємною складовою методології управління ризиками інформаційної безпеки громади є антикризові комунікації. Відсутність ефективної комунікації може призвести до поширення панічних настроїв, дезінформації та втрати довіри до місцевої влади. З цієї причини ефективна система управління ризиками інформаційної безпеки повинна включати чіткі механізми інформаційної взаємодії з мешканцями в кризових умовах.

Таким чином, методологія управління ризиками інформаційної безпеки територіальної громади повинна розглядатися як комплексна система організаційних, технічних, кадрових та комунікаційних заходів, спрямованих на своєчасне

виявлення, оцінювання, попередження та мінімізацію інформаційних загроз. Її ефективне впровадження дозволить забезпечити стабільність роботи органів місцевого самоврядування, підвищити рівень цифрової стійкості громади та сформувати безпечне інформаційне середовище в умовах сучасних викликів і цифрової трансформації.

Список використаних джерел:

1. Богач Ю. Цифровізація діяльності органів місцевого самоврядування як інструмент забезпечення сталого розвитку територіальних громад. *Економічний простір*. 2025. № 201. С. 264-268 URL: https://economic-prostir.com.ua/article/201-czyfrovizacziya-diyalnosti-organiv-misczevogo-samovryaduvannya-yak-instrument-zabezpechennya-stalogo-rozvytku-terytorialnyh-gromad/
2. Василенко В.М. Громади як суб'єкти кібербезпеки: просвітництво, моніторинг і відповідальність у цифровому середовищі. *Вісник Харківського національного університету внутрішніх справ.* 2025. №111 (4), С. 469-483. DOI: https://doi.org/10.32631/v.2025.4.38.
3. Лєнков О.С. Напрями формування інформаційних механізмів антикризового управління розвитком територіальних громад в Україні. *Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування».* 2025. Вип. 33 (62). С. 275-291. URL: https://ojs.uem.edu.ua/index.php/spnma/article/view/871/1876