Олег БОГАЧ
аспірант кафедри менеджменту,
публічного управління та персоналу
Західноукраїнського національного університету

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК НЕВІД'ЄМНА СКЛАДОВА ВІДНОВЛЕННЯ ТА РОЗВИТКУ ТЕРИТОРІАЛЬНИХ ГРОМАД

В умовах трансформаційних процесів, що відбуваються в Україні та світі, інформаційна безпека дедалі більше набуває стратегічного значення, стаючи однією з ключових передумов ефективного функціонування, відновлення та довгострокового розвитку територіальних громад. Цифровізація системи публічного управління, автоматизація адміністративних процедур, розвиток цифрових платформ взаємодії між владою, населенням і бізнесом значно розширили можливості територіальних громад в контексті забезпечення якісного надання послуг, підвищення прозорості управлінських процесів, оперативного прийняття рішень та активізації громадської участі. Водночас зростання рівня цифрової залежності громад супроводжується підвищенням вразливості до широкого спектра інформаційних загроз, що робить питання інформаційної безпеки не допоміжним технічним компонентом, а фундаментальним елементом стійкості місцевих систем управління.

В цуй самий час – в умовах воєнного стану та повоєнного відновлення України, територіальні громади одночасно одночасно повинні забезпечувати роботу базових публічних сервісів, підтримки соціальної стабільності, здійснювати управління ресурсами, організовувати координацію гуманітарної допомоги та реагувати на кризові виклики. Тобто, інформаційний простір стає не лише середовищем управлінської взаємодії в громаді, а й об’єктом потенційних деструктивних впливів, включаючи кібератаки, спроби дестабілізації цифрових сервісів, витік конфіденційної інформації, інформаційно-психологічні операції та маніпулятивне поширення дезінформації. Тому інформаційну

безпеку доцільно розглядати не лише як складову кіберзахисту, а як комплексний управлінський механізм забезпечення безперервності функціонування громади, захисту критичних даних, підтримання довіри населення до місцевої влади та створення передумов для стабільного розвитку.

Беззаперечно, що сучасна територіальна громада працює з великою кількістю різної інформації. Це дані про бюджет, управлінські рішення, соціальні послуги, стан інфраструктури, звернення громадян, роботу комунальних служб, а також персональні дані мешканців. Для ефективної роботи управлінням активно використовуються цифрові інструменти, серед яких: електронний документообіг, онлайн-послуги, ЦНАП-сервіси, електронні платформи для звернень громадян, системи моніторингу інфраструктури та інші. Завдяки цьому місцева влада може швидше приймати рішення, краще взаємодіяти з мешканцями, бізнесом, державними органами та міжнародними партнерами. Водночас чим більше громада залежить від цифрових систем, тим вищими стають ризики. Тому завдання місцевої влади полягає не лише у захисті комп'ютерних систем, а й у запобіганні ризикам, які можуть порушити її роботу. Наприклад, збій у роботі електронних реєстрів, систем документообігу або платформ надання адміністративних послуг може ускладнити доступ людей до необхідних сервісів, затримати прийняття управлінських рішень та створити хаос у роботі громади. З цієї причини забезпечення інформаційної безпеки ми розглядаємо як необхідну складову ефективного управління, особливо в умовах криз, воєнних загроз та повоєнного відновлення.

Однією з серйозних проблем для територіальних громад стає зростання кіберзагроз. Органи місцевого самоврядування дедалі більше використовують цифрові технології у своїй роботі, тому все частіше стають цілями кібератак. Такі атаки можуть бути спрямовані на викрадення інформації, блокування роботи електронних сервісів, пошкодження важливих баз даних або порушення роботи технічних систем. Особливо небезпечними є

ситуації, коли атака зачіпає ЦНАП, системи електронного документообігу, фінансові сервіси, офіційні канали комунікації чи об'єкти критичної інфраструктури, від яких залежить нормальне функціонування громади.

Важливо зазначити, що суттєвими загрозами для територіальних громад є не лише кібератаки, а й витік персональних даних та поширення неправдивої або маніпулятивної інформації. Органи місцевого самоврядування працюють із великою кількістю інформації про мешканців, соціальні виплати, медичні й адміністративні послуги, бюджетні ресурси та інші. Тому неналежний захист такої інформації може призвести до серйозних проблем, втрати довіримешканців до влади та створити соціальну напругу. Також небезпеку становлять і поширювані фейки, дезінформація, які можуть дезорієнтувати населення, викликати недовіру до місцевої влади та ускладнити прийняття важливих рішень, особливо у кризових ситуаціях. Саме тому інформаційна безпека сьогодні є важливою складовою загальної безпеки громади, так само як економічна, соціальна чи інфраструктурна безпека. Для її ефективного забезпечення недостатньо лише технічного захисту комп'ютерних систем – потрібен комплексний підхід, який поєднає сучасні технології, чіткі правила роботи з інформацією, належну організацію процесів та підготовку працівників.

Виходячи з цього вважаємо, що ефективний захист інформації в територіальній громаді повинен базуватися на комплексному підході. Насамперед важливо, щоб у громаді були чітко визначені правила роботи з інформацією, розподілена відповідальність між працівниками, зрозумілі дії у разі виникнення загроз чи технічних збоїв, а також постійний контроль за можливими ризиками. Важливу роль при цьому має відігравати і технічний захист, а саме використання сучасних програм безпеки, резервного збереження даних, захисту доступу до систем та інших цифрових інструментів, які допомагають запобігти втраті або викраденню інформації. Проте навіть найкращі технології не гарантують повного захисту, якщо працівники не знають основ безпечної роботи з інформацією

або допускають помилки. З цієї причини важливими є регулярне навчання персоналу та розвиток цифрової грамотності. Не менш значущою є ефективна комунікація з мешканцями, адже громада повинна швидко надавати достовірну інформацію, спростовувати фейки та підтримувати довіру населення. Найбільш результативним підходом у цьому напрямку є багаторівневий захист, коли безпека забезпечується не одним окремим інструментом, а кількома взаємопов'язаними рівнями захисту.

Таким чином, інформаційна безпека в сучасних умовах повинна розглядатися як невід'ємна складова відновлення та розвитку територіальних громад, що поєднує технічний, управлінський, соціальний і стратегічний виміри. Її забезпечення є не лише реакцією на сучасні загрози, а й інвестицією у стійкість, керованість, конкурентоспроможність та довгострокову спроможність громади до розвитку.