Філонов М.В.,
аспірант,
Класичний приватний університет
(м. Запоріжжя, Україна)

ПІДХОДИ ДО ВДОСКОНАЛЕННЯ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА РЕГІОНАЛЬНОМУ РІВНІ

Сучасне безпекове середовище України формується під впливом гібридної війни, розпочатої рф. Однією з ключових складових цієї війни є інформаційно-психологічні операції, спрямовані на дестабілізацію ситуації в регіонах України [1]. Особливо вразливими є території з високим рівнем інформаційної залежності від зовнішніх джерел, низькою медіаграмотністю населення та слабкою інституційною спроможністю.

У Стратегії інформаційної безпеки України (2021 р.) підкреслено необхідність розбудови інформаційної стійкості на місцевому рівні як частини загальнодержавної системи [2]. У той же час, реалізація цієї стратегії не позбавлена недоліків, що позначаються на існуючій системі публічного управління інформаційною безпекою в регіонах, а саме:

1. Фрагментованість нормативно-правової бази у сфері забезпечення інформаційної безпеки регіонів. Відсутність уніфікованої законодавчої політики щодо інформаційної безпеки на регіональному рівні призводить до нерівномірного впровадження стандартів.
2. Недостатня координація між центром і регіонами в питаннях забезпечення інформаційної безпеки. Непоодинокими є випадки, коли відсутні ефективні управлінські механізми передачі повноважень, фінансування і відповідальності у сфері кібербезпеки на місця.
3. Кадровий голод. Брак кваліфікованих ІТ-спеціалістів в органах державної влади та місцевого самоврядування ускладнює реалізацію регіональних стратегій захисту інформації на місцях.
4. Недовіра громадян до цифрових сервісів. Зниження рівня цифрової довіри уповільнює процес впровадження новітніх технологій у публічне адміністрування.

Незважаючи на наявність базових інституційних (що включають правові й організаційні) механізмів публічного управління, реалізація інформаційної політики на регіональному рівні залишається недостатньо ефективною. Серед основних викликів можемо визначити такі:

– фрагментарність відповідальності між органами виконавчої влади, органами місцевого самоврядування та силовими структурами [3];

– низький рівень готовності місцевих влад до інформаційних криз [4];

– обмеженість правового регулювання питань інформаційної безпеки саме на регіональному рівні.

Відповідно до наукових досліджень у сфері публічного управління [5; 6] удосконалення системи інформаційної безпеки на регіональному рівні вимагає інтеграції таких управлінських підходів і методів:

1. Системного, що передбачає забезпечення єдності організаційної, нормативної та технічної інфраструктури.

2. Проактивного, який передбачає аналітичну роботу з ідентифікації потенційних загроз ще до їх реалізації.

3. Інклюзивного, орієнтованого на залучення громадськості та ЗМІ до процесу формування політики.

4. Цифрового, що включає впровадження інтелектуальних систем виявлення фейкових новин, координацію через цифрові платформи.

На наше переконання, удосконалення правового й організаційного механізмів публічного управління у сфері інформаційної безпеки на регіональному рівні можливе за умови:

– розробки регіональних стратегій інформаційної безпеки відповідно до Державної стратегії кібербезпеки [7]. Очевидно, що гібридна війна рф, що ведеться проти України, актуалізує питання щодо визначення ролі регіональних стратегій у забезпеченні інформаційної безпеки. Регіональні стратегії мають бути орієнтовані на адаптацію до специфіки місцевих викликів. Це вимагає створення локальних центрів кіберзахисту, розробки освітніх програм для підвищення цифрової грамотності публічних службовців і громадян, упровадження інструментів е-демократії з високим рівнем захисту персональних даних;

– упровадження інформаційних радників або аналітичних центрів при ОВА;

– розбудови інфраструктури моніторингу інформаційного простору із залученням наукових і громадських інституцій [8].

Крім того, вищевказані механізми публічного управління повинні бути інтегровані у системи кризового управління та регіональні програми цифрової трансформації [9].

Щодо прикладів успішного досвіду регіонального менеджменту інформаційної безпеки, то можна навести такі:

1) проект “Фільтр” від ГО “Інтерньюз-Україна”, впроваджений у Чернігівській області, що включав онлайн-моніторинг фейків і навчання місцевих чиновників [10];

2) ініціативи з підвищення медіаграмотності у школах Львівської та Сумської областей;

3) партнерство Дніпропетровської ОДА з кіберполіцією у сфері моніторингу соцмереж під час виборів [11].

Отже, розбудова ефективної системи публічного управління у сфері інформаційної безпеки на регіональному рівні є ключовою умовою протидії гібридним загрозам. Скоординована діяльність держави, місцевої влади, громадянського суспільства та експертного середовища здатна забезпечити сталу стійкість до інформаційних атак і сформувати адаптивну, безпечну інформаційну екосистему.

Список використаних джерел:

1. Цибулько В. Інформаційна війна як складова гібридної агресії: виклики для України. *Наукові записки Інституту політичних і етнонаціональних досліджень.* 2020. № 2. С. 45–51.
2. Стратегія інформаційної безпеки України. Указ Президента України №685/2021 від 14 травня 2021 року. URL: https://www.president.gov.ua/documents/6852021-41069
3. Державна служба спеціального зв'язку та захисту інформації України. Звіт про стан кіберзахисту в Україні за 2023 рік. URL: https://cip.gov.ua/ua/news/2023-roku-kilkist-zareyestrovanikh-kiberincidentiv-zrosla-na-62-5-zvit-operativnogo-centru-reaguvannya-na-kiberincidenti-dckz.
4. Власюк О. Системні загрози інформаційній безпеці в умовах гібридної війни. *Національна безпека і оборона*. 2022. № 3. С. 11–18.
5. Дейнека О. Концептуальні підходи до формування стійких систем публічного управління. *Державне управління: теорія та практика.* 2021. № 1.
6. Васильченко В. Механізми публічного адміністрування інформаційною безпекою: сучасний стан та перспективи розвитку. *Вісник НАДУ*. 2022. № 4. С. 27–33.
7. Стратегія кібербезпеки України на 2021–2025 рр. Затверджена Указом Президента №447/2021 від 26 серпня 2021 р. URL: https://www.president.gov.ua/documents/4472021-40013.
8. Renz B. Information Warfare and Russia's Strategy. Routledge, 2020.
9. Мінцифри про результати цифрової трансформації в регіонах України за 2024 рік. URL: https://oda.zht.gov.ua/news/mintsyfry-pro-rezultaty-tsyfrovoyi-transformatsiyi-v-regionah-ukrayiny-za-2024-rik/.
10. ГО «Інтерньюз-Україна». Проєкт «Фільтр». URL: https://internews.ua/filter.
11. Кіберполіція України. Офіційний звіт про співпрацю з регіонами у сфері кіберзахисту – 2023. URL: https://cyberpolice.gov.ua.