ПУБЛІЧНЕ УПРАВЛІННЯ В СИСТЕМІ НАЦІОНАЛЬНОЇ КІБЕРБЕЗПЕКИ: ВИКЛИКИ ГІБРИДНОЇ ВІЙНИ ТА НАПРЯМИ АДАПТАЦІЇ

Гончарук Юрій Володимирович

здобувач освітньо-наукової програми доктора філософії за спеціальністю «Публічне управління та адміністрування» кафедри публічного управління та адміністрування Національного лісотехнічного університету України.

Забезпечення стійкості державного управління в умовах війни та конфліктів є критично важливим завданням для будь-якої країни.

В сучасних умовах є необхідність комплексного застосування сучасних форм і методів інформаційного забезпечення діяльності органів влади. В основному, це стосується новітніх інформаційних технологій для підтримки прийняття рішень з метою забезпечення ефективного функціонування системи публічного управління.

Україна постійно стає об’єктом численних гібридних загроз і вже більше 11 років протистоїть російській агресії. В зв’язку з цим постає критична необхідність в якісній підготовці кадрів для державної служби для ефективної протидії таким загрозам. Публічні управлінці є мішенню як для кіберзлочинів, так і для інформаційно-психологічних операцій, що вимагає комплексного підходу до їхньої навчання.

В умовах сучасного безпекового середовища гібридні загрози стали одними із найсерйозніших викликів для національної безпеки. Ці загрози поєднують військові та невійськові методи: інформаційні атаки, економічний тиск, кібероперації тощо.

НАТО вже давно визнало кіберпростір п’ятою окремою, специфічною та важливою сферою ведення збройної боротьби, поряд із чотирма традиційними — «Земля», «Море», «Повітря» та «Космос» [1].

Європейський центр передового досвіду з протидії гібридним загрозам (Hybrid CoE), визначає, що «гібридні загрози – це скоординовані та синхронізовані дії, які навмисно спрямовані на системні вразливості демократичних держав та інститутів за допомогою широкого спектру засобів» [2].

Складність сучасних загроз вимагає превентивних дій та скоординованих зусиль на світовому та регіональному рівнях. Основні види актуальних гібридних загроз перелічено в таблиці 1.

Таблиця 1

Види гібридних загроз та їхні особливості

№ з/п	Види гібридних загроз	Особивості
1.	Кіберзагрози	Кібероперації, що спрямовані на підрив критичної інфраструктури, крадіжку даних і порушення функціонування державних інституцій
2.	Інформаційні війни	Маніпуляція суспільною думкою, дезінформація та пропаганда, що підривають довіру до влади та збройних сил
3.	Економічний тиск	Використання економічних важелів для дестабілізації економіки країни, блокування торгівлі та інвестицій
4.	Нерегулярні збройні формування	Використання нерегулярних збройних угруповань, що діють на території країни з метою дестабілізації та підриву територіальної цілісності.

Складено автором за даними [1].

Для протидії гібридним загрозам необхідно реформування інституцій та налагодження міжвідомчої взаємодії. В Україні вже створюються спеціалізовані підрозділи, які займаються протидією гібридним загрозам, кібербезпекою та інформаційною боротьбою. Це дозволяє підвищити ефективність протидії цим викликам. Іншим важливим елементом протидії є зміцнення взаємодії між відомствами для їх тісної координації.

Водночас ці зміни є недостатніми без формування базового розуміння кіберзагроз публічними управлінцями. Вони повинні бути обізнаними з найбільш поширеними видами загроз, такими як фішинг, соціальна інженерія, шкідливе програмне забезпечення (Malware) тощо. Для цього необхідно регулярно проводити навчання і короткі інтерактивні тренінги.

Цілями атак може бути отримання доступу до конфіденційної інформації, порушення нормального функціонування певних сервісів та надання послуг, маніпуляції з даними тощо. Як правило, подібні атаки реалізуються через некомпетентність деяких працівників. Саме людський фактор, а точніше нехтування чи відсутність розуміння базових правил безпечної роботи з інформаційними системи та інформацією призводить до проблем.

Публічні управлінці повинні чітко розуміти як діяти в разі виявлення підозрілих ситуацій чи кіберінцидентів, а також коли і як залучати фахівців з кібербезпеки. Для ефективного управління подібними ситуаціями необхідно чітко розмежовувати відповідальності публічного управлінця та технічного фахівця. Завданням управлінця є не безпосереднє технічне втручання, а організація процесу реагування, яка має бути спрямована на ухвалення обґрунтованих рішень, що базуються на аналізі ризиків та даних, наданих експертами з кібербезпеки. У той час як фахівці проводять ідентифікацію, стримування та ліквідацію загрози, управлінець координує процес відновлення сервісів, організовує комунікацію (зокрема із засобами масової інформації) та забезпечує взаємодію зі слідчими органами. Саме тому програми навчання для держслужбовців повинні включати

також вивчення правової бази та процедурних аспектів розслідування кіберзлочинів, включаючи правила збереження цифрових доказів.

Україна вже зараз активно працює над підвищення рівня кібербезпеки на державному рівні. 14 квітня 2025 року відбулося засідання Національного координаційного центру кібербезпеки. На ньому було ухвалено низку стратегічних рішень, спрямованих на посилення кіберстійкості України. Серед яких наступні:

- створення та забезпечення функціонування єдиної інфраструктури для обробки, передавання та зберігання даних, необхідних для держави;
- запровадження вимог до операторів (державних, комунальних, приватних), які надають послуги зі зберігання даних, а також механізмів аудиту;
- обов'язкове розміщення резервних копій державних електронних інформаційних ресурсів і баз даних на території України та під її юрисдикцією, зокрема у національних хмарних сервісах; забезпечення належного резервування критичних даних на національному рівні [3].

Вказані вище заходи значною мірою сфокусовані на впровадженні технічних рішень. Не зважаючи на їхню важливість, вони можуть мати обмежену ефективність проти атак, спрямованих на використання людського фактора. В зв'язку з цим слід розглянути також заходи, орієнтовані на підвищення рівня кіберсвідомості та формування базових безпекових компетенцій у державних службовців, зокрема:

- Впровадження регулярних тренінгів, орієнтованих на розвиток практичних навичок ідентифікації актуальних кіберзагроз (зокрема, різних форм фішингу), засвоєння протоколів безпечної роботи з даними та протидії психологічним маніпуляціям.
- Періодичне проведення симуляцій кібератак публічних управлінців, зокрема тестових фішингових розсилок. Їхні результати повинні стати основою для подальшого коригування тренінгових програм.

- Проведення регулярних інформаційних кампаній з метою підтримки високого рівня обізнаності щодо нових загроз та найкращих практик захисту.

Поєднання вказаних вище заходів із вже існуючими технічними засобами захисту здатне суттєво зміцнити кібербезпеку державних установ та критичної інфраструктури в Україні. Це особливо важливо за постійних кібератак в умовах війни.

Список використаних джерел:

1. Підготовка кадрів для протидії гібридним загрозам: Україна на шляху до євроатлантичних стандартів. УКРАЇНА В НАТО. 06.05.2024. URL: https://ukrainetonato.com.ua/75-rokiv-nato/pidhotovka-kadriv-dlia-protydii-hibrydnym-zahrozam-ukraina-na-shliakhu-do-yevroatlantychnykh-standartiv/ (дата звернення: 13.10.2025).

2. Hybrid threats as a concept. Hybrid CoE. URL: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (дата звернення: 12.10.2025).

3. Кібератака на Мін'юст і «Укрзалізницю», цифровий суверенітет України: Відбулося засідання НКЦК. Рада національної безпеки і оборони України : офіц. сайт. 14.04.2025. URL: https://www.rnbo.gov.ua/ua/Diialnist/7154.html (дата звернення: 13.10.2025).