

ПАРАДИГМИ ГІБРИДНОГО ВПЛИВУ В ІНФОРМАЦІЙНІЙ СФЕРІ НА ПРИКЛАДІ ДЕРЖАВНО-УПРАВЛІНСЬКИХ ЗАСАД

Перевертай В.О., НУЦЗУ

НК - Хмиров І.М., доктор наук з державного управління, доцент НУЦЗУ

В сучасних державно-управлінських реаліях постає очевидним той факт, що дійсно існує низка викликів, що виникають у сучасному нестабільному безпековому середовищі, яке характеризується, перш за все, дедалі більш розмитою відмінністю між війною та миром, що впливає на всі сфери державної політики, у тому числі й на державну інформаційну політику. У цьому природно складному та дедалі неоднозначному середовищі концепції гібридних загроз і гібридної війни допомагають як у структуруванні розуміння природи загроз, з якими ми стикаємося, так і в стратегії та методах потенційних супротивників. Таким чином, слід використовувати комплексний погляд на загрози, а також на існуючі інструменти та засоби протидії їм. Такий комплексний погляд акцентує увагу на природі загроз і супротивників, а також викликах, які вони створюють для демократичних країн. При цьому стає все більш важливим питання спроможності демократій та демократичних державних інституцій безпеки протистояти гібридним загрозам і гібридній війні, розуміючи конкретні вразливі місця в демократичних суспільствах і ліквідуючи їх, а також розробляючи відповіді на ворожі заходи з боку зовнішніх акторів. Особлива вразливість і обмеження, а також переваги демократій вимагають особливих підходів у цьому середовищі. Відкриті суспільства, побудовані на нормативних засадах верховенства права, прав людини та демократії, обов'язково захищаючи свободу слова, об'єднань і преси, повинні розробити рішення, які не тільки зберігають ці основні свободи, але й спираються на їхні сильні сторони. Як показує досвід багатьох країн, ця робота йде повним ходом, для чого залучаються численні організації, яким доручено аналізувати та вирішувати проблему протидії гібридним загрозам, у тому числі (а часто і переважно) в інформаційній сфері [2].

Враховуючи складний характер наявних загроз, реагування має бути організованим відповідно спільних принципів, інтегруючи різні сектори суспільства, а також різні держави. Ще один важливий висновок, який випливає з розглянутого вище, це важливість знання свого противника. У той час як ідентифікація та приписування загроз створює реактивні відповіді, проактивне усунення наявних вразливостей для підвищення стійкості вимагає усвідомлення не лише того, що робить супротивник, але й чому. У зв'язку з цим актуальним стає погляд на світ очима супротивника, щоб визначити стратегічні цілі та шляхи їх досягнення, а також уразливі місця супротивника [1].

ЛІТЕРАТУРА

1. Khriapynskiy A., Khmyrov I., Svoboda I., Shevchuk M., Iastrebova V. State information security strategies in conditions of hybrid threats. Amazonia Investiga. Vol12 (No69), 84-93.
2. Хряпинський А. П., Хмиров І.М. Парадигми гібридного впливу в інформаційній сфері на прикладі державно-управлінських засад. Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування. Вип. № 9. 2023.