ПРОТИДІЯ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

Ангеліна КУЗЬМІН

Ростислав ТКАЧУК

Валерія БАЛАЦЬКА

У сучасному цифровому світі захист інформаційного простору є одним із ключових чинників національної безпеки. Зростання кіберзагроз, поширення дезінформації та активний розвиток штучного інтелекту створюють нові виклики, що суттєво ускладнюють протидію маніпуляціям та інформаційним атакам.

Сучасні інформаційні впливи виявляються у вигляді дезінформації, компрометації та свідомого спотворення фактів. У науковій літературі визначено, що інформаційно-психологічна операція – це цілеспрямована діяльність, спрямована на зміну поведінки та світогляду цільових груп задля досягнення стратегічних цілей. Близьким поняттям є психологічна війна, що передбачає систематичне використання пропаганди та інших засобів впливу для досягнення переваг у міжнародних відносинах.

В умовах цифровізації особливої ролі набувають інтернет і соціальні мережі як інструменти інформаційної війни. Технології Web 2.0 та Web 3.0 забезпечують можливості для маніпуляцій через таргетований контент, SMM-кампанії, використання бот-мереж, фейкових акаунтів, створення діпфейків і психологічних портретів користувачів.

Важливою складовою сучасних інформаційних війн є кібернетичні атаки – навмисні дії, спрямовані на порушення конфіденційності, цілісності та доступності інформаційних ресурсів. Вони здійснюються у формі DDoS-атак, фішингу, упровадження шкідливого програмного забезпечення, зламів вебресурсів, а також втручання у роботу критичної інфраструктури.

Сучасні інформаційні конфлікти мають виражений мережевий характер, поєднуючи онлайн- і офлайн-інструменти. Їхнє завдання полягає у зміні суспільної свідомості, контролі над інформаційним простором, впливі на політичні процеси та стратегічні рішення. Для досягнення цілей застосовуються технології контент-менеджменту, персонального брендингу, вірусного маркетингу, моніторинг та аналіз інформаційних потоків.

Відповідно до Стратегії інформаційної безпеки України інформаційна загроза визначається як потенційно або реально негативні явища в інформаційній сфері, що здатні унеможливити реалізацію національ-

них інтересів. Окрему увагу документ приділяє інформаційним операціям рф, спрямованим на дестабілізацію суспільно-політичної ситуації в Україні. Основними механізмами протидії визначено застосування санкцій, розвиток системи стратегічних комунікацій та підвищення рівня медіаграмотності населення. До 2025 року планується створення захищеного інформаційного простору, протидія незаконному контенту та забезпечення реінтеграції громадян на тимчасово окупованих територіях.

Світова практика демонструє різноманітні підходи до боротьби з дезінформацією. У Німеччині діє законодавство, яке зобов'язує соціальні мережі видаляти протиправний контент у встановлені строки. У Франції ухвалено закон про протидію маніпуляціям інформацією, що передбачає швидкий розгляд позовів щодо поширення фейків. Європейський Союз формує експертні групи, розробляє критерії виявлення фейкових новин і системи оперативного попередження.

Серед основних методів виявлення дезінформації виокремлюють аналіз джерел, вивчення стилістики подання матеріалів, перевірку фактів і використання спеціалізованих платформ (FactCheck.org, Snopes). Значну роль відіграють технологічні підходи, зокрема алгоритми машинного навчання: наївний метод Баєса, метод опорних векторів, нейронні мережі.

Для ефективної протидії необхідно поєднувати законодавчі ініціативи, технічні рішення у сфері кібербезпеки, розвиток критичного мислення та медіаграмотності громадян. Важливим залишається міжнародне співробітництво, обмін досвідом і швидке реагування правоохоронних органів. Лише комплексний підхід може забезпечити надійний захист інформаційного простору держави.