DOI https://doi.org/10.36059/978-966-397-570-2-127

Таран Є. І.,
кандидат політичних наук, доцент,
доцент кафедри глобальної та національної безпеки
Київського національного університету імені Тараса Шевченка
м. Київ, Україна

ВИКЛИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНОМУ ПРОСТОРУ УКРАЇНИ **В УМОВАХ ГІБРИДНОЇ ВІЙНИ**

Інформаційна політика держави є невід'ємною складовою національної безпеки, на неї покладено визначення механізмів створення, поширення і, перш за все, захисту інформації, в умовах сучасних викликів. Ефективне управління інформаційними потоками відіграє важливу роль в питаннях збереження стабільності держави, підтримці її демократичних інститутів та захисті національних інтересів.

З огляду на гібридні загрози, Україна змушена зміцнювати інформаційну безпеку як складову загальної стратегії національної безпеки. Інформаційні атаки, маніпуляції громадською думкою, кібератаки та використання інформаційних технологій у військових конфліктах потребують комплексного й системного підходу до формування державної інформаційної політики.

Основу ефективного функціонування інформаційної політики складає законодавство, що регулює питання забезпечення інформаційної безпеки. Так, в Україні розроблено та ухвалено низку нормативно-правових актів, які регулюють інформаційний простір. Перш за все – це Закон України «Про національну безпеку України» [3]. Він визнає інформаційну безпеку однією з важливих складових національної безпеки. У Законі України «Про інформацію» [2] визначено правові засади доступу до інформації, її поширення та захисту.

В той же час, існуюча законодавча база потребує подальшого покращення відповідно до сучасних викликів та загроз. Перш за все, необхідно розширити механізми протидії дезінформації, здійснити впровадження ефективних стратегічних комунікацій та провести заходи по зміцненню кібербезпеки при активному застосуванні цифрових технологій у гібридних війнах.

В умовах інформаційної війни держава повинна зменшувати шкоду від інформаційних атак противника, використовуючи контратаки та результативно застосовуючи свої комунікаційні засоби для здійснення контрпропаганди. В рамках внутрішньої інформаційної політики держава повинна викривати ворожу пропаганду, швидко реагувати на неправдиві інформаційні повідомлення, спростовуючи їх,

що повинно призводити до запобігання реалізації противником своїх завдань [1, с. 126].

Інформаційний простір України наразі перебуває під впливом численних серйозних викликів, які безпосередньо загрожують національній безпеці. Серед ключових проблем – поширення дезінформації та маніпулятивних матеріалів, що мають на меті розхитати суспільну стабільність, підірвати довіру громадян до державних органів та спровокувати антиурядові настрої. Додаткову небезпеку становлять кіберзагрози та атаки хакерів, спрямовані на порушення роботи важливих інформаційних систем, таких як державні реєстри, банківська інфраструктура, енергетичні об'єкти та засоби зв'язку. Подібні дії можуть мати суттєві негативні наслідки для безпеки країни та її економічної стабільності.

Разом з тим, соціальні мережі набули значного значення як інструмент цілеспрямованого інформаційного впливу. Ворог активно використовує ці платформи для поширення неправдивих повідомлень, пропагандистських матеріалів і ворожих наративів, застосовуючи алгоритми для точного націлювання на окремі групи населення з метою формування потрібних настроїв. Паралельно з цим, зовнішні інформаційні втручання через підконтрольні медіа-ресурси здатні трансформувати політичний дискурс у державі, маніпулюючи суспільною думкою та сприяючи зміні пріоритетів у громадських настроях.

З метою ефективного протистояння сучасним інформаційним загрозам, державна інформаційна політика має бути орієнтована на розробку та впровадження нормативно-правових механізмів, які дозволять здійснювати належний контроль над інформаційним середовищем та забезпечувати протидію деструктивним впливам, зокрема поширенню дезінформації. Водночас державні інституції повинні мати достатній потенціал для оперативного реагування на будь-які інформаційні виклики. У цьому контексті особливого значення набуває розвиток систем моніторингу та швидкого реагування на спроби інформаційних маніпуляцій.

У контексті сучасних інформаційних загроз критично важливим є зміцнення кібербезпеки, розвиток національної кіберінфраструктури та формування спеціалізованих структур, відповідальних за захист державних інформаційних ресурсів. Ці заходи є ключовими для забезпечення надійного функціонування державних систем і гарантування національної безпеки в умовах зростаючого цифрового тиску. Активна співпраця з міжнародними партнерами дозволяє обмінюватися досвідом, координувати дії для протидії кіберзагрозам і забезпечувати глобальну кібербезпеку [4].

Держава повинна адаптувати свою інформаційну політику до тих викликів, що існують в міжнародному інформаційному середовищі та у сфері забезпечення інформаційної безпеки. Ефективна адаптація

інформаційної політики вимагає модернізації правових та організаційних механізмів управління інформаційною безпекою.

Список використаних джерел:

1. Горун О. Ю. Протидія ворожій медіа-пропаганді в умовах правового режиму військового стану в Україні. *Інформація і право.* 2023. № 1(44). С. 116–128. URL: https://ippi.org.ua/sites/default/files/12_27.pdf

2. Про інформацію: Закон України від 15.11.2024 № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

3. Про національну безпеку України: Закон України від 09.08.2024 № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

4. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України. Державне управління*. 2019. Вип. 3. URL: https://periodica.nadpsu.edu.ua/index.php/governance/article/view/296/297