Список використаних джерел

1. Задорожній О.В. Інформаційне право України: навч. посіб. / О.В. Задорожній. К. : Юрінком Інтер, 2015. 272 с.
2. Лисенко В.І. Свобода слова та інформаційна безпека: баланс інтересів / В. І. Лисенко // *Вісник Національної академії правових наук України.* 2019. № 4. С. 115–125.
3. Цимбалюк В. Права людини в інформаційному суспільстві / В. Цимбалюк // *Право України.* 2020. № 1. С. 43–50.
4. Кушнарьова І.В. Правове регулювання свободи слова в Україні: монографія / І.В. Кушнарьова. Х. : Право, 2017. 320 с.
5. Костенко Н., Мельник О. Інформаційна безпека та гібридні загрози: аналіз сучасних викликів / Н. Костенко, О. Мельник // *Науковий вісник Інституту інформаційного суспільства.* 2021. № 2. С. 21–29.
6. Центр стратегічних комунікацій та інформаційної безпеки. Інформаційна боротьба РФ проти України: ключові наративи [Електронний ресурс]. Режим доступу: https://spravdi.gov.ua/
7. Різун В.В. Інформаційна безпека в системі національної безпеки України: навч. посіб. / В.В. Різун. К. : Інститут журналістики КНУ імені Тараса Шевченка, 2010. 176 с.

Кривенко Валерія Вадимівна,
ад'юнкт кафедри теорії, історії та філософії права Національної академії внутрішніх справ

ПРЕВЕНТИВНА КОМУНІКАЦІЯ ЯК ІНСТРУМЕНТ ПРОТИДІЇ ІНФОРМАЦІЙНИМ ЗАГРОЗАМ

У сучасному глобалізованому інформаційному середовищі інформаційні загрози набувають нових форм і масштабів, стаючи одним із головних інструментів гібридних впливів, маніпуляцій громадською думкою та підриву національної безпеки. У цьому контексті превентивна комунікація виступає як стратегічний інструмент, що дозволяє не лише реагувати на інформаційні атаки, а й попереджати їх, зменшуючи їхню ефективність ще на етапі формування.

Превентивна комунікація – це комплексна система заходів інформаційного впливу, спрямованих на запобігання виникненню конфліктів, деструктивних суспільних процесів, поширенню дезінформації та фейків. Вона передбачає не лише інформування, але й активну взаємодію з громадянами, формування довіри до державних інституцій, насамперед поліції.

Інформаційна загроза – потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України

і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні [1]. Таке розуміння інформаційної загрози фактично вказує на її складний системний характер, що проявляється у формі цілеспрямованого негативного впливу на свідомість, поведінку та інститути суспільства, становить реальну або потенційну загрозу національній безпеці держави. Її наслідки проявляються у підриві демократичних процесів, дестабілізації внутрішнього середовища та послабленні обороноздатності. Відповідно, враховуючи стратегічну важливість інформаційного простору, ефективне виявлення, нейтралізація та превенція таких загроз має розглядатися як пріоритетна складова державної політики у сфері національної безпеки, що потребує науково обґрунтованого підходу, міжвідомчої координації та високого рівня інформаційної культури суспільства.

Сьогодні збройна агресія російської федерації проти України є не лише воєнним конфліктом у традиційному розумінні, а й масштабною гібридною війною, де інформаційний компонент відіграє критично важливу роль. Інформаційні загрози в цьому контексті не лише супроводжують бойові дії, а й формують окремий фронт, спрямований на підрив морального духу населення, дестабілізацію державного управління, ослаблення міжнародної підтримки та легітимацію агресії в очах як власної, так і іноземної аудиторії.

Збройна агресія рф спричинила інтенсивне зростання кількості та складності інформаційних загроз, зокрема:

- фейкові новини та дезінформація;

Дезінформація – це недостовірна, оманлива, маніпулятивна інформація, створена навмисно заради отримання економічних, політичних або інших вигод, а фейкові новини є одним із методів її поширення. Фейковим новинам притаманні такі риси як неправдивий маніпулятивний зміст; спрямованість на навмисне введення в оману, дезорієнтацію споживача; подання інформації від імені хибних або анонімних джерел; використання чуток та сатири; поширення в мережі Інтернет; економічні або політичні мовити створення [2, с. 183].

- пропагандистські кампанії активізувались у вигляді системної державної політики рф. Вони спрямовані на створення «альтернативної реальності», demonізацію України, виправдання агресії, зокрема через міфи про «визвольну місію» [3].
- кібератаки синхронізуються з військовими діями. Зокрема, у перші дні вторгнення у лютому 2022 року було зафіксовано масові кібератаки на урядові ресурси України, що супроводжували фізичний наступ.
- інформаційно-психологічні операції (ІПСО);

Інформаційно-психологічні спеціальні операції (далі – *ІПСО*) – це комплекс заходів щодо поширення спеціально підготовленої інформації з метою впливу на емоції, почуття та поведінку людей [4, с. 189]. Необхідно погодитись з М. Савлюком, який наголошує на тому, що ІПСО в соціальних мережах стали ключовим елементом гібридної війни проти України. Сьогодні можна виділити такі організаційні аспекти проведення ІПСО:

- створення мереж ботів і фейкових акаунтів;
- використання лідерів думок та псевдо експертів;

– координація дій через закриті групи та канали;
– застосування технологій глибинних шейків;
– використання алгоритмів соціальних мереж для посилення ефекту [5, с. 303; 6].

В умовах збройної агресії рф зазвичай ІПСО спрямовані на деморалізацію українського суспільства, посів паніки та підрив довіри до владних інституцій.

➢ deepfake-технології.

Дипфейк (від deep learning – глибинне навчання нейронних мереж і fake – підробка) – це технологія створення фальсифікованого, але візуально правдоподібного контенту, яка є новітньою формою онлайн-дезінформації. Його особливістю є можливість достатньо переконливо імітувати реальні, наприклад, відео, при цьому глядач може сумніватися у власному сприйнятті. Створення дипфейків може здійснюватись на основі поєднання голосу однієї особи із зображенням або відео іншої. У результаті формується реалістичний фальшивий відеозапис, на якому начебто виступає справжня людина. У більшості випадків у глядача не виникає підозри щодо фейковості побаченого [7, с. 74].

Наукові дослідження свідчать, що в умовах гібридної війни інформаційний фронт є критично важливим для досягнення стратегічних цілей противника. Згідно з висновками Національного інституту стратегічних досліджень, інформаційні впливи мають на меті трансформацію поведінки соціуму, вплив на ухвалення політичних рішень та деморалізацію військових структур [8]. Відповідно, це вимагає системного посилення національної інформаційної безпеки, розвиток стратегічної комунікації, підвищення критичного мислення та медіаграмотності суспільства.

Одним із ключових інструментів у протидії інформаційним загрозам є превентивна комунікація, зокрема і здійснювана з боку правоохоронних органів. Адже вона дозволяє формувати стійкість суспільства до маніпуляцій, забезпечує довіру до офіційних джерел і знижує рівень паніки та дезінформації.

Превентивна комунікація являє собою перш за все стратегію інформаційного впливу, яка має на меті:

– *попередження конфліктів* – інформування про потенційні ризики та конфліктогенні фактори, що можуть призвести до загострення ситуації або ескалації насильства;

– *зниження напруги*, зокрема, шляхом поширення інформації, що сприяє розумінню і співпраці між різними групами населення, що допомагає знижувати соціальну та політичну напругу;

– *інформування населення* – надавання точних і достовірних відомостей про права людини, заходи безпеки і можливості отримання допомоги в умовах воєнного конфлікту [9, с. 31-32].

Успішна протидія інформаційним загрозам потребує від органів влади, зокрема і поліції, переходу від реактивної до проактивної моделі дій. Йдеться про системне використання таких інструментів превентивної комунікації, як:

– *взаємодія з місцевими громадами*. Зокрема, поліцейські, постійно перебуваючи в певному районі, формують зв’язки з мешканцями, ідентифікують проблемні зони та разом із громадою шукають шляхи їх вирішення. Така модель

дозволяє не лише швидко реагувати на правопорушення, а й запобігати їм завдяки зміцненню довіри до поліції [10].

– медіаосвіта: навчання громадян критичному мисленню та перевірці джерел інформації. Працівники поліції систематично проводять заходи у навчальних закладах, робочих колективах, громадах – тренінги, лекції, майстер-класи щодо правової обізнаності, кібербезпеки, ненасильницького вирішення конфліктів тощо [11].

– інформаційні кампанії: створення контенту, спрямованого на розвінчання міфів і протидію пропаганді. Так, у своїй діяльності поліція активно використовує соціальні платформи (Facebook, Twitter, Instagram, YouTube) для інформування громадськості, спростування фейків, поширення рекомендацій, а також встановлення зворотного зв'язку з населенням. Цифрові канали комунікації створюють можливість для оперативного інформування про загрози та попередження злочинів [12].

– технологічні рішення: використання ІКТ для захисту інформації, наприклад, шифрування даних і моніторингу кіберпростору [13].

Прикладом ефективного використання інструментів превентивної комунікації є діяльність підрозділів комунікації Національної поліції України, зокрема у періоди соціальної напруги, терористичних загроз або масових заходів. Вчасна, правдива та цільова комунікація у таких випадках сприяє зниженню рівня паніки, протидії дезінформації та посиленню авторитету поліції.

Незважаючи на ефективність превентивної комунікації, її впровадження, зокрема з боку поліції, стикається низкою структурних, технологічних і суспільних бар'єрів. Зокрема, недостатня цифрова грамотність населення призводить до порушення ними правил кібергігієни. В свою чергу, недостатня кількість поліцейських, які належно володіють інструментами цифрової комунікації та кризових комунікацій, не дозволяє здійснювати ефективну превентивну діяльність у цьому напрямі, особливо на деокупованих територіях. Також, необхідно погодитись з Ю.В. Шевченко, який наголошує на тому, що відсутність системи моніторингу ІПСО та оперативного реагування на ворожі меседжі створює суттєві ризики для суспільної довіри [14].

Існує потреба у формуванні належної взаємодії між усіма органами державної влади, зокрема і поліцією, оргранами місцевого самоврядування, медіа та громадськими організаціями. Доцільно, на наш погляд, створити постійно діючі платформи такої взаємодії.

Підсумовуючи вищевикладене, необхідно зазначити, що превентивна комунікація є ефективним інструментом протидії інформаційним загрозам, що дозволяє мінімізувати вплив дезінформації, пропаганди та кібератак. Вона ґрунтується на освітніх, організаційних і технологічних заходах, які забезпечують інформаційну безпеку та стійкість суспільства. Для успішної реалізації превентивної комунікації необхідно посилити цифрову грамотність громадян, удосконалити організаційно-технічну модель кіберзахисту. Доцільно здійснити інституційну реформу комунікаційної функції органів влади, зокрема і поліції, створити сталі партнерства із громадськими та медійними структурами тощо.

Список використаних джерел

1. Стратегя інформаційної безпеки України: Указ Президента України від 21 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text
2. Тищенко В.С., Мужанова Т.М. Дезінформація і фейкові новини: ознаки та методи виявлення в мережі Інтернет. *Кібербезпека: освіта, наука, техніка.* 2022. № 2 (18). С. 175-186. URL: https://csecurity.kubg.edu.ua/index.php/journal/article/view/413/341
3. Pomerantsev, P. This Is Not Propaganda: Adventures in the War Against Reality. London : Faber & Faber, 2019. 288 p.
4. Бартельова А., Рудь О. Інформаційно-психологічні операції як основна загроза інформаційній безпеці держави. / Протидія дезінформації в умовах російської агресії проти України: виклики і перспективи. Харків, 2023. С. 188-190. URL: https://www.researchgate.net/publication/376773925_Informacijno-psihologicni_operacii_ak_osnovna_zagroza_informacijnij_bezpeci_derzavi
5. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету.* Серія: Політологія. 2024. Випуск 18. С. 300-309. URL: https://journals.pnu.if.ua/index.php/politology/article/view/167/164
6. Благодарний А.М., Штельмах О.В. Організаційні аспекти протидії інформаційній агресії як складовій гібридної війни. *Інформаційна безпека людини, суспільства, держави.* 2015. № 3. С. 48–54.
7. Доскіч Л.С. Фейкові новини як новітній засіб маніпуляції та дезінформації. *Бібліотекознавство. Документознавство. Інформологія.* 2022. № 4. С. 72–77.
8. Національний інститут стратегічних досліджень. Превентивна комунікація як елемент інформаційної політики держави. URL: https://niss.gov.ua
9. Кривенко В.В. Роль превентивної комунікації у забезпеченні прав людини в умовах збройного конфлікту. / Актуальні питання становлення та розвитку сучасного конституціоналізму в Україні: матеріали науково-практичного столу (Київ, 28 червня 2024). 2024. 87с. С. 31-33. URL: https://elar.navs.edu.ua/server/api/core/bitstreams/6c086bb4-2a42-4a9a-9728-3b09c99d6e2a/content
10. Войтович, О.М. Community policing як складова запобігання злочинності в Україні. *Право і безпека*. 2021. № 2. С. 37–42.
11. Антонюк, А.В. Освітні ініціативи поліції як засіб профілактики правопорушень серед молоді. *Юридичний вісник України*. 2020. № 4. С. 52–58.
12. Науменко, Д.І. Комунікаційна стратегія Національної поліції у соціальних мережах. *Інформаційне суспільство*. 2022. № 3. С. 28–33.
13. Яремчук Ю.Є., Павловський П.В., Катаєв О.В. Комплексні системи захисту інформації. Вінниця: ВНТУ, 2023. URL: https://web.posibnyky.vntu.edu.ua
14. Шевченко, Ю.В. Стратегії протидії ІПСО в діяльності правоохоронних органів. *Сучасні інформаційні технології і суспільство*. 2023. № 2. С. 66–72.