

4. Як хактивісти змінюють природу соціальних протестів. *Український тиждень*. веб-сайт. URL : <https://tyzhden.ua/iak-khaktyvisty-zminiuiut-pryrodu-sotsialnykh-protestiv/>

5. Anonymous: історія створення та успіху «Анонімус». *WorldBank*. веб-сайт. URL : <https://worldbank.org.ua/4616-anonymous.html>

6. Даємо 48 годин. Anonymous закликали західні компанії припинити роботу в Росії. *Суспільне новини*. веб-сайт. URL : <https://suspilne.media/amp/220003-daemo-48-godin-anonymous-zaklikali-zahidni-kompanii-priviniti-robotu-v-rosii/>

7. Хактивісти нагадали росіянам, як путін підривав мирних людей 25 років тому. *АрміяInform*. веб-сайт. URL : <https://armyinform.com.ua/2024/09/22/haktyvisty-nagadaly-rosiyanam-yak-putin-pidryvav-myrnyh-lyudej-25-rokiv-tomu/>

8. Хактивісти «Кібер-АТЕШ» вивели з ладу сайт пропагандистського проєкту «Безсмертний полк». *Ukr.net*. веб-сайт. URL : <https://www.ukr.net/news/details/technologies/111210691.html>

9. Українські хактивісти зламали комп'ютер командувача сил РФ на Запорізькому напрямку: побачене шокує (фото, відео). *TSN*. веб-сайт. URL : <https://tsn.ua/ato/ukrayinski-haktivisti-zlamali-komp-yuter-komanduvacha-silami-rf-na-zaporizkomu-napryami-foto-video-2701356.html>

Білодід Катерина Сергіївна,
*курсант навчально-наукового інституту
поліцейської діяльності Національної
академії внутрішніх справ*

СОЦІАЛЬНІ МЕРЕЖІ ЯК ІНСТРУМЕНТ ІНФОРМАЦІЙНОЇ ВІЙНИ: АТАКИ, ФЕЙКИ ТА ПРОТИДІЯ

У сучасному світі соціальні мережі перетворилися на потужний інструмент, що виходить далеко за рамки простого спілкування чи самовираження. Вони стали могутнім важелем впливу на колективну свідомість, формування суспільної думки, поширення інформації, мобілізацію населення, а також організацію як патріотичної активності, так і протестних рухів. Особливої ваги соцмережі набули в умовах гібридної війни, яка поєднує як військові, так і інформаційні аспекти.

Інформаційна війна ґрунтується на цілеспрямованому поширенні фальшивої або маніпулятивної інформації. Її мета – дестабілізувати суспільство, підірвати довіру до державних установ, знизити моральний дух населення та оборонних сил. У цьому контексті соцмережі демонструють свою вразливість: вони слугують ідеальним середовищем для дезінформації завдяки швидкості поширення вмісту, масштабній аудиторії та відсутності належного контролю за достовірністю інформації.

Серед найбільш небезпечних проявів інформаційної війни в соціальних мережах – поширення фейкових новин [1]. Такі повідомлення спеціально створюються або навмисно викривляються, вводячи аудиторію в оману стосовно подій, осіб чи явищ. Щоб ускладнити розкриття фейків, застосовуються хитрощі, зокрема використання стилю офіційних джерел, емоційно насиченої мови, супровід фото- та відеоматеріалами.

Сучасні підходи до ведення інформаційної війни в соціальних мережах включають створення мереж ботів і фейкових акаунтів, маніпуляції через таргетовану рекламу та використання алгоритмів для просування потрібного контенту. Ці технології дозволяють швидко змінювати акценти у публічному дискурсі, відволікати увагу громадськості від важливих питань та формувати вигідне агресорові сприйняття подій.

У відповідь на такі виклики правоохоронні органи повинні адаптувати свою діяльність до реалій інформаційних загроз. Їхня роль сьогодні охоплює не лише забезпечення фізичної безпеки, але й систематичний моніторинг інформаційного простору. Критично важливим стає виявлення джерел дезінформації, ідентифікація осіб, які залучені до деструктивної діяльності, та нейтралізація їхнього впливу [2]. Усе це потребує освоєння нових компетентностей, тісної співпраці з кіберполіцією та Службою безпеки України, а також використання сучасних технологічних рішень.

В Україні зараз діє значна кількість ініціатив, спрямованих на боротьбу з фейками. Це включає платформи перевірки фактів, телеграм-канали для спростування дезінформації, а також кампанії, що популяризують медіаграмотність серед громадян. Однак проблема залишається надзвичайно актуальною через активну діяльність ворожих інформаційних операцій та обмежені можливості для продуктивної протидії.

Ефективна боротьба із поширенням фейкової інформації не обмежується технічними чи репресивними методами [3]. Вона вимагає відкритості державних структур, послідовної роботи з населенням, конструктивного діалогу з медіа та активної участі офіційних джерел у соціальних мережах. Прозора комунікація від імені держави суттєво зменшує вплив панічних настроїв і загрозливих дезінформаційних хвиль.

Окрему увагу потрібно приділяти захисту персональних даних користувачів у соцмережах, оскільки ці дані можуть стати інструментом для маніпуляцій. Їхній витік або незаконне використання створює можливість для цільових інформаційних атак, посилюючи їх ефективність. У цьому ключі надзвичайно важливе правове регулювання та застосування сучасних заходів кібербезпеки. У сучасних умовах роль кіберполіції значно зростає.

Ще однією важливою частиною протидії дезінформації є розвиток інформаційної культури громадян. Медіаграмотність – це вміння критично мислити, перевіряти джерела інформації та розпізнавати ознаки маніпуляцій. Відтак систематична робота у цьому напрямі має зайняти одну з провідних позицій у сферах освіти й професійної підготовки, особливо для фахівців правоохоронної сфери.

Таким чином, соціальні мережі в сучасних умовах війни є важливим інструментом поширення інформації. Їхня експлуатація агресором для поширення фейків, послаблення моралі населення та підризу довіри до правоохоронних органів стала одним із найгостріших викликів сьогодення. Проте саме ці платформи надають державі та громадянському суспільству можливість ефективно взаємодіяти та боротися з інформаційними загрозами.

Список використаних джерел

1. Інформаційні атаки в соціальних мережах: дослідження впливу російської дезінформації через рекламу в Facebook. Центр стратегічних комунікацій та інформаційної безпеки. URL: <https://cedem.org.ua/wp-content/uploads/2024/05/informacziyni-ataky-v-soczialnyh-merezhah.-doslidzhennya-vplyvu-rosijskoyi-dezininformacziyi-cherez-reklamu-v-facebook.pdf> (дата звернення: 16.05.2025).

2. Данько Ю. Соціальні мережі як інструмент інформаційної війни рф проти України: особливості та механізми протидії. *Сучасне суспільство: політичні науки, соціологічні науки, культурологічні науки*. Наукові фахові видання ХНПУ імені Г.С. Сковороди. 2023, Випуск 2 (27). С.54–66. URL: <http://journals.hnpu.edu.ua/index.php/politology/article/view/14247>

3. Савлюк М. Важливість інформаційної безпеки в соціальних мережах для загальнонаціональної безпеки: безпековий вимір України. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. № 18. С.300–309. URL: <https://journals.pnu.if.ua/index.php/politology/article/view/167>

Богдан Ігор Васильович,
аспірант кафедри теорії держави та права Національної академії внутрішніх справ

ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ ОБОРОННОЇ ФУНКЦІЇ УКРАЇНИ В КОНТЕКСТІ ВІДСУТНОСТІ ЧЛЕНСТВА В НАТО

Повномасштабна збройна агресія Російської Федерації проти України, що триває з лютого 2022 року, та пов'язана з нею стратегічна невизначеність щодо термінів і умов набуття Україною повноправного членства в Організації Північноатлантичного договору (НАТО) надають особливої актуальності дослідженню правових засад забезпечення оборонної функції Української держави. За відсутності колективних гарантій безпеки, передбачених статтею 5 Північноатлантичного договору, Україна постає перед унікальними юридичними викликами у реалізації свого невід'ємного суверенного права на оборону. Це вимагає глибокого правового аналізу наявних національних та міжнародно-правових механізмів, що забезпечують цю функцію, а також пошуку шляхів їх посилення.