Колесник Наталія Миколаївна,
курсант ННІ Харківського
національного університету
внутрішніх справ
Науковий керівник:
Калєніченко Лідія Іванівна,
завідувач кафедри інформаційних
систем та технологій Харківського
національного університету
внутрішніх справ, доктор юридичних
наук, професор

ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ТА ІПСО: ВИКЛИКИ ДЛЯ НАЦІОНАЛЬНОЇ БЕЗПЕКИ

В умовах інформаційного суспільства інформація стає найбільш важливим ресурсом, який визначає функціонування та розвиток усіх без виключення сфер суспільного життя. Саме тому у будь-якій діяльності питання інформаційної безпеки є основним фактором, який формує її ефективність.

Важливість інформаційної безпеки ми відчули особливо гостро з початком воєнної агресії росії. Саме в інформаційній сфері ворог поширює величезну кількість шкідливої інформації про нашу державу. Він прагне дезінформувати, послабити, обеззброїти.

Сучасну людину оточує величезний обсяг інформації: соціальні мережі, інформаційні сайти, телебачення та численні месенджери. Одночасно з невпинним зростанням її кількості постійно збільшується число фейків та маніпуляцій. Неправдиву інформацію поширюють для того, аби сформувати у людей хибну картину світу [1, с. 188].

Під час повномасштабного вторгнення українці споживають інформацію більш виважено. Народ України намагається більш критично ставитися до маніпулятивної інформації та навчився краще відрізняти фейк від правди.

Такі дії ворога є прямою загрозою для національної стійкості (резильєнтності) України, яка в політичній науці визначається не лише як здатність держави «вижити», а як спроможність інституцій та суспільства адаптуватися до криз, зберігати ефективність і швидко відновлюватися після інформаційних ударів [2, с. 149].

За своєю суттю ІПСО – це комплексна дезінформація та пропаганда, що базується на навмисному перебільшенні або применшенні певної інформації, а також супроводжується кібератаками та диверсіями на цивільній інфраструктурі. У ширшому розумінні це

справжня психологічна війна, метою якої є формування потрібної ворогу громадської думки через прямий вплив на свідомість.

Науковий підхід до розуміння ІПСО визначає їх як комплекс заходів із поширення спеціально підготовлених даних для керування поведінкою людей. Процес підготовки таких операцій завжди є поетапним та розпочинається з етапу планування, де визначаються цілі, завдання, засоби впливу та конкретна цільова аудиторія. Далі обирається або штучно створюється інформаційний привід, який слугує фундаментом для подальшої операції. На основному етапі цей привід використовується для трансформації або руйнування суспільно-політичних зв'язків, а завершується процес етапом закріплення, що забезпечує сталість досягнутих результатів. Важливо розуміти, що подібні методи використовуються людством тисячоліттями, і змінюються лише технології донесення: якщо раніше це були чутки через торговців, то сьогодні головним інструментом стали соцмережі та анонімні Telegram-канали.

Сучасні технології дозволяють агресору використовувати алгоритми штучного інтелекту та мережі автоматизованих акаунтів (ботоферм) для миттєвого масштабування дезінформації, що створює ілюзію масової підтримки ворожих наративів [3, с. 146].

Кінцевою метою ІПСО завжди є зміна моделі поведінки людини через нав'язування гострих емоцій, таких як страх, злість чи викривлене бажання справедливості, що в результаті підштовхує особу до конкретних вчинків.

При цьому метою операції часто є не лише нав'язування конкретної брехні, а й провокування стану «інформаційного паралічу», коли через надлишок суперечливих даних громадяни перестають довіряти будь-яким джерелам, що руйнує суспільну єдність.

Для ефективної протидії цим загрозам національній безпеці необхідно звертати увагу на ключові маркери ворожого впливу. По-перше, це критична потреба у повному відмежуванні від російського контенту, оскільки ворог діє через мережу блогерів та лідерів думок для легітимізації свого бачення реальності. По-друге, фундаментом безпеки є дотримання інформаційної гігієни, яка мінімізує негативний вплив деструктивних потоків даних на психічне та фізичне здоров'я людини.

Ефективною відповіддю на ці виклики є впровадження стратегії превентивної комунікації, яка дозволяє державі перейти від реактивного реагування на фейки до проактивної моделі дій. Це передбачає не лише вчасне інформування населення про потенційні ризики, а й системну медіаосвіту та використання цифрових платформ для встановлення зворотного зв'язку, що критично важливо для зниження соціальної напруги та зміцнення довіри до офіційних джерел [1].

Такий підхід дозволяє формувати у суспільства своєрідний «інформаційний імунітет», де громадяни стають стійкими до маніпуляцій ще до моменту початку активної фази ворожої атаки.

Такий комплексний підхід до розуміння природи ІПСО дозволяє не лише розпізнавати маніпуляції, а й вибудовувати надійний когнітивний захист у масштабах усієї держави.

Зрештою у сучасній війні кожен цифровий пристрій у руках громадянина є або інструментом оборони, або потенційною вразливістю, що перетворює індивідуальну відповідальність за споживання контенту на невід'ємний елемент колективної безпеки держави

Підсумовуючи вищевикладене, слід зазначити, що інформаційно-психологічні операції в умовах сучасної війни є однією з найсерйозніших загроз національній безпеці України. Вони спрямовані на системну деструкцію суспільної свідомості, руйнування внутрішньої єдності та підрив національної стійкості (резильєнтності). Оскільки методи ворожого впливу постійно еволюціонують – від використання класичної пропаганди до впровадження алгоритмів штучного інтелекту та масових ботоферм – протидія цим загрозам також має бути комплексною та багаторівневою.

Ключем до захисту держави є перехід від простого реагування на ворожі вкиди до стратегії проактивної превентивної комунікації. Це передбачає формування «інформаційного імунітету» населення через розвиток медіаграмотності, дотримання цифрової гігієни та зміцнення довіри між суспільством і державними інституціями. Лише поєднання високої професійної підготовки фахівців зі стратегічних комунікацій та індивідуальної критичної оцінки інформації кожним громадянином дозволить вибудувати надійний когнітивний захист України, здатний протистояти будь-яким викликам гібридної агресії.

Список використаних джерел

1. Бартельова А., Рудь О. Інформаційно-психологічні операції як основна загроза інформаційній безпеці держави. Науково-дослідний інститут публічної політики і соціальних наук. *Протидія дезінформації в умова російської агресії проти України: виклики і перспективи.* Харків, 2023. С. 188–190. URL: https://surl.li/lzxcdb

2. Ульяненко К. В. Інформаційна безпека як фактор формування національної стійкості України. Політичні інститути та процеси. 2025. *ПОЛІТИКУС*. Науковий журнал. С. 148–153. URL: https://politicus.od.ua/2_2025/25.pdf

3. Кривенко В. В. Превентивна комунікація як інструмент протидії інформаційним загрозам. Національна академія внутрішніх справ. 2025. С. 145–149. URL: https://surl.lu/bkexid