DOI: https://doi.org/10.32782/PPSS.2023.1.43

ГАРАНТУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РОСІЙСЬКОЇ АГРЕСІЇ ПРОТИ УКРАЇНИ

Ганна Геннадіївна ТАРАНЕНКО,

канд. політ. наук,
старша викладачка кафедри міжнародних відносин Національного університету "Києво-Могилянська академія", Київ, Україна
https://orcid.org/0000-0003-2588-4941

GUARANTEEING INFORMATION SECURITY UNDER THE RUSSIAN AGGRESSION AGAINST UKRAINE

Information security is one of the important components of guaranteeing national and international security. Challenges to information security in today's world are extremely serious - from cyberattacks and cyberaggression to manipulation of the consciousness of social groups and interference in elections. Guaranteeing Ukraine's information security and developing resilience to information threats is an important dimension of the ongoing Russian-Ukrainian war. The measures should be aimed at both external and internal audiences with appropriate information messages and appeals. The use of successful international experience and the mutually enriching exchange of ideas with international allies and partners are the key to increasing Ukraine's resilience to information challenges under the ongoing Russian aggression.

Інформаційна безпека є однією з важливих складових гарантування національної та міжнародної безпеки. Виклики інформаційній безпеці у сучасному світі є надзвичайно серйозними – від кібератак та кіберагресії до маніпуляцій свідомістю суспільних груп та втручання у вибори. При цьому поняття безпеки можна визначити як збереження норм, правил, інститутів і цінностей суспільства [1, с. 1]. Усі інституції, принципи та структури, пов'язані з суспільством, включаючи його людей, мають бути захищені від "військових і невійськових загроз" [1, с. 1]. Поняття національної безпеки України можна визначити як захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних і потенційних загроз [2, с. 2]. А поняття інформаційної безпеки України можна визначити як складову частину національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом [3, с. 2].

Гарантування інформаційної безпеки України та розвиток стійкості до інформаційних загроз є важливим виміром триваючої російсько-української війни. Інформаційні загрози виступають частиною гібридних засобів ведення війни, які використовує Російська Федерація. При цьому головною метою гібридних засобів ведення війни є спантеличити супротивника і перешкоджати його процесу прийнятті рішень.

З метою введення противника в оману часто використовуються кампанії інформаційного впливу. Зокрема, Шведське агентство з цивільних надзвичайних ситуацій (MSB) виокремлює такі елементи кампанії інформаційного впливу, як

– використання технік впливу: зв'язки з громадськістю, маркетинг, дипломатія, громадська журналістика та лобіювання є прикладами загальноприйнятих способів впливу на погляди та поведінку людей;

– зрив громадських дискусій: іноземні держави використовують інформаційну діяльність, щоб впливати на ті сфери та дебати, з яких вони можуть отримати користь. Це може робитись як прямо, так і опосередковано, за допомогою різних способів: від відкритої пропаганди до прихованого фінансування груп громадянського суспільства;

– дії у власних інтересах: діяльність, спрямована на досягнення конкретних цілей, які приносять користь іноземній державі, при цьому мета може бути будь-якою – від політичної дестабілізації суспільства і перешкоджання прийняттю конкретних рішень до поляризації політичних дебатів;

– використання вразливостей: усі суспільства мають свої виклики. Це можуть бути соціальна чи класова напруженість, нерівність, корупція, питання безпеки чи інші проблеми, які мають центральне значення для суспільного життя. Ворожі іноземні держави виявляють і систематично використовують ці вразливі місця для досягнення своїх цілей [4, с. 12].

Одним з найважливіших завдань для української держави і суспільства є забезпечення інформаційної безпеки в умовах російської агресії. При цьому заходи мають бути спрямовані як на зовнішню, так і на внутрішню аудиторію з відповідними інформаційними посилами та закликами. Використання успішного міжнародного досвіду та взаємозбагачуючий обмін ідеями з міжнародними союзниками і партнерами є запорукою підвищення стійкості України до інформаційних викликів в умовах триваючої російської агресії.

Список використаних джерел:

1. National Security versus Global Security. *United Nations*. URL: https://www.un.org/en/chronicle/article/national-security-versus-global-security (дата звернення: 21.11.2020).

2. Закон України "Про національну безпеку України" (Відомості Верховної Ради (ВВР), 2018, № 31, ст.241). *Верховна Рада України.* URL: https://zakon.rada.gov.ua/laws/show/2469-19. (дата звернення: 21.11.2023).

3. Указ Президента України №685/2021 Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки". *Президент України. Офіційне Інтернет-представництво*. URL: https://www.president.gov.ua/documents/6852021-41069

4. Countering Information Influence Activities. A Handbook for Communicators. *Swedish Civil Contingencies Agency*. URL: https://www.msb.se/RibData/Filer/pdf/28698.pdf.