# ДЕМПФУВАННЯ ВИКЛИКІВ НАЦІОНАЛЬНІЙ БЕЗПЕЦІ УКРАЇНИ В СУЧАСНИХ УМОВАХ

# DAMPING OF CHALLENGES TO UKRAINE'S NATIONAL SECURITY IN MODERN CONDITIONS

УДК 351/354
DOI https://doi.org/10.32782/pma2663-5240-2024.41.24

**Кравченко О.І.**
аспірант кафедри публічного управління та адміністрування
Національний авіаційний університет

**Лелеченко А.П.**
д. наук з держ. упр., професор, професор кафедри публічного управління та адміністрування
Національний авіаційний університет

*Стаття присвячена питанням демпфування загроз національної безпеки України в сучасних умовах. Інформаційне суспільство, яке характеризується інтенсивним обміном інформацією та широким використанням цифрових технологій, відкриває нові можливості, але водночас і нові загрози для національної безпеки. В умовах, коли інформаційні атаки, кіберзагрози та дезінформація стають повсякденними викликами, питання забезпечення національної безпеки набуває критичного значення. Основною метою цього дослідження є аналіз методів та засобів демпфування загроз національній безпеці України в умовах інформаційного суспільства. Демпфування у даному контексті розуміється як процес зменшення впливу негативних чинників на безпеку держави шляхом впровадження комплексних заходів, спрямованих на виявлення, попередження та нейтралізацію загроз. Це включає як технічні засоби захисту інформаційних систем, так і заходи організаційного, правового та освітнього характеру. Сучасні загрози національній безпеці в інформаційному просторі України можна класифікувати на кілька основних категорій: кіберзагрози, інформаційні війни, дезінформація та пропаганда, а також порушення інформаційної безпеки критичних інфраструктур. Кожна з цих категорій має свої особливості та вимагає специфічних підходів до демпфування. Для ефективного демпфування загроз національній безпеці України в сучасних умовах необхідно також удосконалювати нормативно-правову базу, що регулює питання інформаційної безпеки. Це включає прийняття нових законодавчих актів, які б відповідали сучасним викликам, а також гармонізацію національного законодавства з міжнародними стандартами та нормами у сфері кібербезпеки та інформаційної безпеки. Демпфування загроз національній безпеці України в умовах інформаційного суспільства є комплексним завданням, що потребує узгоджених дій з боку держави, приватного сектору та громадянського суспільства.*

**Ключові слова:** *демпфування, національна безпека, інформаційний простір.*

*The article is devoted to the issues of dampening threats to Ukraine's national security in modern conditions. The information society, which is characterized by intensive exchange of information and wide use of digital technologies, opens up new opportunities, but at the same time new threats to national security. In conditions where information attacks, cyber threats and disinformation are becoming daily challenges, the issue of national security becomes critical. The main goal of this study is the analysis of methods and means of dampening threats to the national security of Ukraine in the conditions of the information society. Damping in this context is understood as the process of reducing the impact of negative factors on the security of the state by implementing complex measures aimed at identifying, preventing and neutralizing threats. This includes technical means of protecting information systems, as well as organizational, legal, and educational measures. Modern threats to national security in the information space of Ukraine can be classified into several main categories: cyber threats, information wars, disinformation and propaganda, as well as violations of information security of critical infrastructures. Each of these categories has its own characteristics and requires specific damping approaches. In order to effectively dampen threats to the national security of Ukraine in modern conditions, it is also necessary to improve the legal framework governing information security. This includes the adoption of new legislative acts that would meet modern challenges, as well as the harmonization of national legislation with international standards and norms in the field of cyber security and information security. Damping threats to the national security of Ukraine in the conditions of the information society is a complex task that requires concerted actions by the state, the private sector, and civil society.*

**Key words:** *damping, national security, information space.*

**Вступ.** В умовах інформаційного суспільства демпфування загроз національної безпеки набуває особливого значення, оскільки інформаційні технології та цифрові комунікації стають ключовими елементами як для економічного розвитку, так і для функціонування держави в цілому. Сучасні загрози, зокрема кібертероризм, інформаційні війни та дезінформація, вимагають розробки та впровадження ефективних стратегій захисту.

**Мета статті** полягає в аналізі напрямків демпфування загроз національної безпеки України як пріоритетного завдання для країни в сучасних умовах.

**Аналіз останніх досліджень і публікацій.** Проблема інформаційної безпеки українського суспільства в сучасних умовах російсько-української війни набула гострої актуальності. Питання сутності інформаційної безпеки та інформаційних загроз представлене в наукових працях Нестерович В.[5], Ткачук Т.[6] та ін.

Проблеми правового забезпечення інформаційної безпеки держави розкриваються в наукових працях О. Барабаш, І. Валюшко, Шемчук В.[7] та інших провідних вітчизняних учених у цій галузі. Питання забезпечення кібернетичної безпеки досліджувати такі

науковці: Веселова Л.[1], Гаврильців М. [2], Глушко А. [3], Леоненко Н., Поступна О.[4] та інші. Поряд з грунтовними дослідженнями нагальним залишається необхідність аналізу питань демпфування загроз національної безпеки України.

**Викладення основного матеріалу.** Основні напрямки демпфування загроз національної безпеки передбачають розробку та впровадження національної стратегії кібербезпеки. Прийняття законів та нормативних актів, що регулюють питання кібербезпеки, таких як Закон України «Про основні засади забезпечення кібербезпеки України»[9]. Реалізація державних програм, спрямованих на підвищення рівня кібербезпеки, зокрема підготовка кадрів та створення інфраструктури. Стратегічним документом, який визначає основні напрями, цілі та завдання у сфері забезпечення національної безпеки України на певний період є Стратегія національної безпеки України 2020[11].

Закон України «Про оборону України» регулює питання організації оборони держави, визначає повноваження та функції органів державної влади у цій сфері[10]. З метою реалізації процесів демпфування загроз національної безпеки важливим є впровадження заходів для захисту критичних інформаційних систем та комунікаційних мереж. Використання систем моніторингу та аналізу кіберзагроз для своєчасного виявлення та реагування на інциденти.

В сучасному світі, де інформаційні технології займають центральне місце в усіх аспектах життєдіяльності суспільства, захист критичних інформаційних систем та комунікаційних мереж стає надзвичайно важливим завданням. Критичні інформаційні системи та комунікаційні мережі є основою для функціонування державних органів, економіки, енергетики, транспорту, охорони здоров'я та інших важливих секторів. Їхня вразливість може мати катастрофічні наслідки для національної безпеки, економічної стабільності та громадського порядку. Впровадження заходів для захисту критичних інформаційних систем та комунікаційних мереж є комплексним процесом, який включає технічні, організаційні та правові аспекти, також розробку та впровадження національних стандартів безпеки, розробка методологій оцінки ризиків та впровадження систем управління інформаційною безпекою. В Україні, наприклад, діють стандарти, узгоджені з міжнародними, такі як ISO/IEC 27001, які визначають вимоги до системи управління інформаційною безпекою.

Людський фактор часто є найслабшою ланкою в системі інформаційної безпеки. Тому важливо забезпечити постійне навчання та підвищення кваліфікації персоналу, який працює з критичними інформаційними системами та комунікаційними мережами. Це включає тренінги з питань інформаційної безпеки, моделювання кібератак та навчання методам реагування на інциденти. Захист критичних інформаційних систем вимагає тісної співпраці між державним та приватним секторами. Це передбачає обмін інформацією про загрози та уразливості, спільну розробку та впровадження заходів захисту, а також проведення спільних навчань та тренінгів з питань кібербезпеки. Створення національних центрів кібербезпеки дозволяє координувати зусилля з протидії кіберзагрозам на державному рівні. Такі центри здійснюють моніторинг кіберпростору, аналізують інциденти, надають рекомендації з захисту інформаційних систем та координують заходи реагування на кіберінциденти. В Україні таку функцію виконує Державна служба спеціального зв'язку та захисту інформації (ДССЗЗІ), яка забезпечує координацію зусиль у сфері кібербезпеки.

Кіберзагрози не мають кордонів, тому міжнародна співпраця є необхідним елементом ефективного захисту критичних інформаційних систем. Україна активно співпрацює з міжнародними організаціями, такими як НАТО, ЄС та ООН, в питаннях кібербезпеки. Це включає обмін інформацією, участь у спільних навчаннях та розробку міжнародних стандартів кібербезпеки.

Протидія дезінформації шляхом підвищення медіаграмотності населення є важливим аспектом сучасної інформаційної безпеки. У світі, де потік інформації постійно зростає, а її достовірність часто викликає сумніви, медіаграмотність стає ключовим інструментом для захисту суспільства від маніпуляцій та пропаганди. Дезінформація – це свідоме поширення неправдивої або маніпулятивної інформації з метою введення в оману або впливу на суспільну думку. Вона може бути використана для політичного тиску, економічних маніпуляцій, створення соціальної напруги або дискредитації осіб та інституцій. У світі, де соціальні мережі та цифрові платформи є основними джерелами інформації для багатьох людей, дезінформація має великий вплив. Медіаграмотність –здатність критично аналізувати інформацію, розуміти механізми її створення та розповсюдження, а також усвідомлювати можливі маніпуляції. Підвищення рівня медіаграмотності допомагає людям ідентифікувати дезінформацію, розрізняти факти від думок та оцінювати надійність джерел.

Одним з ефективних способів підвищення медіаграмотності є впровадження освітніх програм та тренінгів. Це можуть бути як курси для школярів та студентів, так і семінари для дорослих. Важливо навчити людей критично мислити, перевіряти джерела інформації, використовувати різні методи перевірки фактів та розуміти основні принципи журналістики. Медіа та журналісти відіграють ключову роль у протидії дезінформації, у разі якщо відповідально підходять до своєї роботи, перевіряють факти, уникають поширення неперевіреної інформації та розкривають маніпуляції. Також важливо підтримувати незалежні та професійні медіа, які можуть служити надійними джерелами інформації.

Сучасні технології пропонують різноманітні інструменти для перевірки фактів, такі як спеціальні платформи, які аналізують достовірність новин та виявляють фейкову інформацію. Використання таких інструментів може значно підвищити ефективність боротьби з дезінформацією.

Громадські організації та активісти також важливий суб'єкт у підвищенні медіаграмотності населення. Вони можуть проводити кампанії з інформування, організовувати тренінги та семінари, співпрацювати з міжнародними партнерами для обміну досвідом та ресурсами, оскільки дезінформація часто поширюється через глобальні мережі.

Розвиток інститутів фактчекінгу в боротьбі з фейковими новинами наступний елемент сучасної інформаційної екосистеми. У світі, де поширення недостовірної інформації може мати серйозні наслідки для суспільства, політики та економіки, фактчекінг стає ключовим інструментом для забезпечення інформаційної безпеки та підтримки демократичних процесів. Фактчекінг – процес перевірки фактів та заяв на предмет їхньої достовірності та точності. Ця практика спрямована на виявлення неправдивої інформації, помилок або маніпуляцій у публічних заявах, новинах та інших джерелах інформації. Фактчекінгові організації працюють над тим, щоб забезпечити суспільство достовірною та перевіреною інформацією. Історія розвитку фактчекінгу розпочата з початку 2000-х років, коли зростання цифрових медіа та соціальних мереж значно ускладнило контроль за достовірністю інформації. Перші організації, такі як FactCheck.org та PolitiFact, з'явилися у США і швидко здобули популярність завдяки своїй незалежності та професіоналізму. Сьогодні фактчекінг є глобальним явищем, з організаціями, що діють у різних країнах світу.

**Висновки.** Загалом, демпфування загроз національної безпеки в умовах інформаційного суспільства потребує системного підходу, що включає правові, технологічні, освітні та міжнародні компоненти. Це забезпечить стійкість держави до сучасних викликів та збереження її суверенітету в умовах глобалізації та цифровізації. У сучасному інформаційному суспільстві, де інформація та комунікаційні технології відіграють вирішальну роль, демпфування загроз національної безпеки стає пріоритетним завданням для України. Аналіз основних аспектів цієї проблематики дозволяє зазначити, що в умовах інформаційного суспільства загрози національній безпеці набувають нових форм. Кіберзлочинність, кібератаки, дезінформація та інформаційні війни стають реальними викликами, які потребують негайного реагування. Україна, як і багато інших країн, стикається з необхідністю адаптувати свої системи безпеки до цих нових загроз. Захист критичних інформаційних систем та комунікаційних мереж є фундаментально важливим для забезпечення національної безпеки. Необхідно розвивати національні стандарти безпеки, впроваджувати сучасні технології захисту, такі як шифрування, аутентифікація та системи виявлення вторгнень. Створення національних центрів кібербезпеки, які координують зусилля в цій сфері, є також важливим кроком. Протидія дезінформації вимагає підвищення рівня медіаграмотності населення та розвитку інститутів фактчекінгу. Освітні програми, тренінги та активна участь громадянського суспільства у перевірці фактів сприяють зменшенню впливу фейкових новин та маніпуляцій. Підтримка незалежних медіа та забезпечення їхньої відповідальності перед суспільством є ключовими факторами успішної боротьби з дезінформацією.

Ефективне демпфування загроз національної безпеки можливе лише за умови тісної співпраці між державним та приватним секторами. Обмін інформацією про загрози, спільні тренінги та навчання, а також розробка спільних заходів захисту є необхідними для створення надійної системи безпеки.

Використання сучасних технологій, включаючи штучний інтелект, машинне навчання та автоматизовані системи аналізу даних, може значно підвищити ефективність заходів з кібербезпеки та протидії дезінформації. Інвестиції у дослідження та розробки в цій сфері мають стати пріоритетом для держави.

**ЛІТЕРАТУРА:**

1. Веселова Л. Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади : монографія / Л. Ю. Веселова ; Одес. держ. ун-т внутр.

справ. – Одеса : Гельветика, 2020. – 486 с. – Бібліогр.: с. 413–486.

2. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. Юридичний науковий журнал. 2020. № 2. С. 200-203.

3. Глушко А.Д., Пантась В.В., Бабенко С.Р. Інформаційна політика в системі забезпечення фінансової безпеки держави. URL: http://www.economy.nayka.com.ua/pdf/2_2022/97.pdf (дата звернення: 02.07.2024).

4. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. Вісник Національного університету цивільного захисту України. Сер.: Державне управління. 2022. Вип. 2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883(дата звернення: 02.07.2024).

5. Нестерович В. Забезпечення інформаційної безпеки як функція держав в умовах сучасних викликів і загроз. Filosofs'ki ta metodologicni problemi prava. 2020. № 1 (19). С. 136-137.

6. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ : Вид. дім «АртЕк», 2018. 411 с.

7. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз: монографія. Київ: Ліра-К, 2020. 352 с.

8. Roubanis, I. Russia's Invasion in Ukraine: the Geopolitical Significance of the War's Impact on Regional Supply Chains (Online): https://fpc.org.uk/wp-content/uploads/2023/07/28072023-Russias-invasion-of-Ukraine-The-geopolitical-significance-of-the-wars-impact-on-regional-supply-chains.pdf (дата звернення: 02.07.2024).

9. Захист інформаційної безпеки як функція держави. URL: http://www.mego.info (дата звернення: 02.07.2024).

10. Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/show/964-15) (дата звернення: 01.07.2024).

11. Стратегія національної безпеки України 2020; (https://zakon.rada.gov.ua/laws/show/392/2020) (дата звернення: 01.07.2024).

12. Закон України «Про оборону України» (https://zakon.rada.gov.ua/laws/show/1932-12) (дата звернення: 02.07.2024).