УДК 004:351.865(477)
DOI https://doi.org/10.32782/ln.2023.20.20

Кобко Є. В.
доктор юридичних наук, доцент
професор кафедри публічного управління
та адміністрування
Національна академія внутрішніх справ
ORCID: 0000-0002-3121–0823

ІНФОРМАЦІЙНА ВІЙНА ТА ДЕЗІНФОРМАЦІЯ: ВПЛИВ НА НАЦІОНАЛЬНУ БЕЗПЕКУ УКРАЇНИ

Аналіз досліджень. Наукова спільнота України відзначена значним обсягом досліджень у сфері інформаційної війни та дезінформації, особливо в контексті їх впливу на національну безпеку. У результаті творчої активності ряду науковців, таких як В.Ю. Артемов, В.О. Хорошко, Ю.Є. Хохлачова, В.В. Погорелов, Ю.Ф. Кучеренко, О.В. Александров, А.М. Носик, Д.О. Камак, Є.В. Курінний, І.М. Сопілко, О.С. Щербіна, М.В. Корнієнко, О.В. Кузьменко, та інших, було здійснено значний прогрес у розумінні та аналізі проблем даної тематики. Дослідження засвідчили, що інформаційна війна є складним явищем, включаючи різноманітні форми інформаційного впливу на суспільство та політику. Враховуючи швидкий розвиток методів ведення інформаційної війни, дане явище потребує детального дослідження, в тому числі в науково-правовому полі, з метою виокремлення ефективних засобів протидії.

Предмет дослідження. Предметом дослідження є інформаційна війна як комплексне явище, її характеристики, методи застосування дезінформації, мотивації та цілі застосування інформаційних загроз, що несуть руйнівні наслідки для стабільності політичної системи, довіри до державних інституцій, економічної безпеки та міжнародних відносин України. Особлива увага приділяється розробленню стратегій та заходів протидії інформаційним загрозам з метою забезпечення національної безпеки країни.

Постановка завдання. Розмаїття інтернет-платформ, соціальних мереж та цифрових медіа створюють унікальні можливості для розповсюдження дезінформації, фейкових новин, та маніпуляційної інформації. Це може призвести до дестабілізації суспільства, порушення довіри до державних інституцій та ескалації конфліктів. Активне використання інформаційної війни стає сучасним інструментом для досягнення політичних, економічних та геополітичних цілей.

Україна, знаходячись у геополітично важливому регіоні, стає об’єктом інформаційних атак, спрямованих на дестабілізацію держави та підрив її суверенітету. Російська агресія та інформаційна війна стали частою реальністю, яка загрожує національній безпеці України.

В умовах такої складної ситуації, розкриття суті інформаційної війни та дезінформації, аналіз їхніх методів та наслідків, стає надзвичайно актуальним завданням. Саме через усвідомлення інформаційних загроз та розробку стратегій протидії дезінформації можна ефективно забезпечити національну безпеку.

Окрім того, зростаюча потреба у співпраці з міжнародними партнерами з метою обміну досвідом та розвитку спільних стратегій протидії інформаційним загрозам вимагає глибокого дослідження та обґрунтування висновків у статті.

Виклад основного матеріалу. Сучасний світ стикається зі складними викликами та

загрозами, серед яких особливої уваги заслуговує інформаційна війна та дезінформація. Ці явища стали ключовими факторами, що впливають на національну безпеку багатьох країн, включаючи Україну. Розповсюдження фейкових новин, маніпуляційна інформація та інформаційні атаки мають потужний вплив на суспільство, політичні структури, економіку та міжнародні відносини. Активна роль технологій та інтернет-платформ створює нові можливості для швидкого поширення дезінформації та зміни публічного дискурсу. Інформаційні атаки можуть мати далекосяжні наслідки, такі як дестабілізація суспільства, порушення довіри до державних інституцій та сприяння розширенню конфліктів.

Україна, яка знаходиться у складному геополітичному контексті, стала об'єктом інформаційних атак, спрямованих на підрив її суверенітету та національної єдності. Російська агресія та інформаційна війна стали не тільки реальними викликами, але й завдали серйозних пошкоджень національній безпеці країни. У цьому контексті, розуміння сутності інформаційної війни та дезінформації, вивчення їх методів та наслідків, а також розробка стратегій протидії стає критичним завданням для національної безпеки України.

Понятійна категорія «інформаційна війна» досліджувалась різними науковцями, проте особливу увагу її визначенню в науково-правовому полі приділяли останні сім-вісім років, оскільки саме в цей період інформаційна війна набула свого особливого значення та стала все частішим різновидом ведення війни, як правило в контексті гібридної війни.

Б.С. Льюїс, наприклад, розглядав «інформаційну війну» в широкому та вузькому сенсі. Згідно першого підходу науковця, вона представляє собою змагання за контроль над інформаційними та комунікаційними процесами, що бере свій початок із самого появи людського спілкування та конфліктів. В світлі іншого, вузького підходу, інформаційна війна полягає у широкомасштабному використанні руйнівної сили проти різних інформаційних систем та активів, включаючи комп'ютери та комп'ютерні мережі, що використовуються для функціонування основних критичних інфраструктур. Більш конкретно, Льюїс вказує на чотири ключові сфери: зв'язок, фінансову, транспортну та електросистему, які виступають основними військовими цілями держави-агресора, що і є ініціатором інформаційної війни, а тому дані сектора потребують особливої уваги з боку національної безпеки [1, с. 1].

На думку О.С. Щербіної, інформаційна війна у своєму класичному тлумаченні передбачає ідеологічну та психологічну маніпуляцію збройних сил, населення та військово-політичного керівництва противника. Її мета – створити сприятливу громадську думку, відповідну власним інтересам, або навіть здійснити дезінформацію з метою нав'язування своєї політичної волі супротивній стороні. Значення терміну «інформаційна війна», як зазначає О.С. Щербіна, може бути розглянуто і в широкому сенсі, включаючи воєнні дії, де використовуються інформаційні технології та засоби. У цьому широкому розумінні, інформаційна війна може охоплювати різноманітні активності, пов'язані з маніпуляцією інформацією для досягнення визначених цілей у воєнних конфліктах та протистояннях [2, с. 311–312].

Обидва науковця погоджуються на тому, що інформаційна війна є певною активністю противника-агресора, що полягає в здійсненні сукупності заходів ідеологічно-психологічного характеру з використанням новітніх інформаційних технологій з метою встановлення контролю над громадською думкою населення та штучного створення недовіри населення до політичної еліти.

Відтак, інформаційна війна – це форма конфлікту та змагання, в якій сторони використовують інформаційні технології, засоби комунікації та медіа з метою досягнення своїх політичних, економічних або військових цілей. Як вже зазначалося раніше, основною метою інформаційної війни є вплив на

громадську думку, психологію та поведінку населення, збройних сил та політичних лідерів противника, що дозволяє досягти стратегічних переваг і перемоги. Така форма конфлікту передбачає наявність певних засобів впливу, які в силу постійного розвитку інформаційних технологій, не можуть бути вичерпними.

І.М. Сопілко зазначає, що основною метою інформаційної війни є послаблення матеріальних та моральних ресурсів противника, одночасно зміцнюючи власні позиції. У ході інформаційної війни агресор здійснює низку дій: поширює страх та панічні настрої серед населення супротивника, використовує дезінформацію для дезорієнтації противника, провокує зміну цінностей та звичаїв іншого народу, змушує владу країни-жертви робити небажані рішення [3, с. 110].

Дана правова позиція знаходить все більше підтверджень в науково-правовому полі, оскільки аналіз існуючої картини ведення війни багатьох країн світу демонструє обов'язкове застосування інформаційних технологій задля досягнення цілої низки стратегічних цілей. Інформаційна війна стала неодмінною складовою сучасного світу, де інформація є потужним знаряддям впливу та контролю. За допомогою інформаційних технологій та масової комунікації, досить незначні дії можуть викликати значний вплив на суспільство та міжнародні відносини.

Сьогоднішні реалії показують, що інформаційна війна може мати далекосяжні наслідки, такі як: знищення довіри громадськості до владних структур, інституцій та засобів масової інформації; поширення ненависті та нетерпимості між національними, етнічними чи релігійними групами; дестабілізація соціально-політичної ситуації в країні або регіоні; зміна геополітичних орієнтирів та національних інтересів країн; вплив на результати виборів та прийняття стратегічних рішень. Популяризація та розповсюдження фейків, спотворення фактів та дезінформація можуть серйозно підривати довіру громадян до інформації, що надходить до них. Це створює ідеальні умови для зловживання та маніпулювання настроями суспільства, а також збільшує ризик конфліктів та зіткнень.

Головним методом ведення інформаційної війни є дезінформація. Загалом, під «дезінформацією» розуміють широкий спектр методів та засобів, що використовуються для свідомого розповсюдження хибних повідомлень, перекрученої інформації або неправдивих даних з метою вводу в оману громадськості або політичних опонентів [4, с. 77]. Проте, деякі науковці визначають «дезінформацію» як поширення публічної інформації, яка містить неправдиві дані і не пройшла перевірку, або була виявлена як неправдива, та може призвести до негативних наслідків для реалізації конституційних прав громадян та загрожувати національній безпеці [5, с. 18].

На думку Таркіна В.П., дезінформацію можна класифікувати за її тривалістю та рівнем організаційної підготовки на разову та тривалу. Такі підвиди будуть мати різні негативні наслідки та, як правило, будуть застосовуватися в контексті відмінних стратегічних цілей. Так, разова дезінформація зідно Таркіна В.П. пов'язана із конкретною ситуацією, подією або окремою особою, і часто поширюється у вигляді чуток або неперевіреної інформації. Тривала або систематична має місце тоді, коли організовані та заплановані заходи застосовуються для введення в оману великих груп людей або цілого населення. Цей рівень дезінформації вищий, він вимагає значного рівня підготовки, координації та ресурсів. Така дезінформація може бути використана для спотворення політичних процесів, впливу на державну безпеку та міжнародні стосунки [6, с. 269].

Незалежно від тлумачення, «дезінформація» носить негативний характер для тої країни, до якої застосовується. У контексті національної безпеки, дезінформація може стати важливим інструментом гібридних загроз, які використовуються для зниження стабільності, національної єдності та влади держави.

Вищевикладене дозволяє дійти до висновку, що інформаційна війна становить серйозну загрозу національній безпеці. Як зазначають, Данільян О. Г., Дзьобань О. П., Панов М. І., забезпечення інформаційної безпеки стає невід'ємною частиною стратегічних зусиль для забезпечення національної безпеки держави. Центральним елементом такої політики повинна стояти системна превентивна діяльність органів державного управління, спрямована на надання гарантій інформаційної безпеки для особистості, соціальних груп, суспільства та держави в цілому [7, с. 158].

Підтримуючи наведену думку, Олег Панченко наголошує на тому, що політика інформаційної безпеки має на меті забезпечення гарантій інформаційного суверенітету України та інформаційної безпеки всіх суб'єктів сфери інформатизації. Її завданням є створення системного підходу до захисту національних інтересів у сфері інформації та задоволення інформаційних потреб суб'єктів національної безпеки [8, с. 8].

Це означає, що політика інформаційної безпеки повинна передбачати впровадження ефективних заходів для запобігання інформаційним загрозам, таким як дезінформація, кібератаки та інші форми інформаційних агресій. Важливо забезпечити надійний захист інформаційної інфраструктури країни та забезпечити безпеку в обміні інформацією між державними органами та громадськістю.

Окрім того, політика інформаційної безпеки повинна сприяти розвитку інформаційної грамотності серед населення, підвищенню свідомості про інформаційні загрози та способи їх протидії. Наукова діяльність у галузі інформаційної безпеки має бути спрямована на пошук нових технологій та методів захисту інформації, а також на аналіз і прогнозування інформаційних ризиків.

Така політика покликана забезпечити стійкий інформаційний простір країни, що є важливою передумовою для зміцнення національної безпеки та захисту національних інтересів. Реалізація такої політики сприятиме підвищенню рівня інформаційної безпеки суспільства та забезпечить стійкий розвиток країни у сучасному цифровому світі.

Висновки. Інформаційна війна та дезінформація є складними та актуальними явищами, які створюють серйозні виклики для національної безпеки України. В контексті сучасного світу, де інформаційні технології та медіа відіграють вирішальну роль у поширенні і впливі інформації, інформаційна війна стає ефективним інструментом для досягнення політичних, економічних та військових цілей.

Зазначені загрози демонструють необхідність ретельного вивчення та аналізу даної проблематики для розробки та впровадження ефективних заходів протидії. Важливо визначити стратегічні підходи до захисту інформаційної інфраструктури країни, забезпечити правовий захист інформаційної безпеки та залучити суспільство до активної участі у цьому процесі.

Розробка превентивних заходів, спрямованих на попередження дезінформаційних кампаній та інформаційних загроз, має бути базовим принципом у діяльності органів державного управління. Потрібно надавати пріоритетний статус створенню і вдосконаленню механізмів реагування на інформаційні атаки та кризових ситуацій.

Зокрема, варто активно впроваджувати програми з підвищення інформаційної грамотності серед населення, зокрема молоді, щоб забезпечити вміння критично оцінювати отриману інформацію та впізнавати дезінформацію. Крім того, сприяти розвитку наукових досліджень у галузі інформаційної безпеки та сприяти обміну знаннями і досвідом з іншими країнами є ключовими кроками для зміцнення інформаційної безпеки України.

Надзвичайно важливо, щоб державна політика інформаційної безпеки була спрямована на створення стійкого інформаційного простору, який би відповідав національним інтересам та вимогам у сфері безпеки. Розуміння принципів та наслідків інформаційної війни,

а також застосування ефективних технологій та методів захисту інформації є важливою передумовою для ефективного протидії дезінформації та забезпечення стійкого розвитку держави.

Таким чином, забезпечення інформаційної безпеки є однією з найважливіших складових національної безпеки України, і лише за умови системного та комплексного підходу можна ефективно протистояти інформаційним загрозам та забезпечити стабільність та процвітання країни в епоху цифрових викликів.

Список використаних джерел:

1. Lewis B.C. Information Warfare. Intelligence Resource Program. The Final Report of the Snyder Commission Edited by Edward Cheng and Diane C. Snyder Woodrow Wilson School Policy Conference 401a: Intelligence Reform in the Post-Cold War Era The Woodrow Wilson School of Public and International Affairs Princeton Unversity. January 1997. URL: https://irp.fas.org/eprint/snyder/infowarfare.htm
2. Щербіна О.С. Інформаційні війни і безпека інформації. Матеріали наукової конференції професорсько-викладацького складу, наукових працівників і здобувачів наукового ступеня за підсумками науково-дослідної роботи за період 2019–2020 рр. (квітень – травень 2021 р.). Вінниця: Донецький національний університет імені Василя Стуса, 2021. 385 с.
3. І.М. Сопілко. Інформаційна війна проти України та правові засоби протидії злочинним діям. Проблеми формування та реалізації державної політики у сфері інформаційної безпеки України. *Юридичний вісник* 3 (64). 2022. С. 108–115. URL: DOI: 10.18372/2307-9061.64.16897
4. Політологія: сучасні терміни і поняття. Короткий навчальний словник-довідник для студентів ВНЗ I–IV рівнів акредитації. 4-тє видання, виправлене і доповнене / укладач В. М. Піча ; наук. редакція Л.Д. Климанської, Я.Б. Турчин, Н. М. Хоми. Львів : Новий Світ – 2000, 2015. 516 с.
5. Фейки, пропаганда, дезінформація та виборчий процес: як нам захистити демократичні практики? / за заг. ред. Д.В. Дубова Київ : ТОВ «Видавництво Сталь», 2019. 254 с. URL: https://ekmair.ukma.edu.ua/server/api/core/bitstreams/a48cdda6-3710-4d9f-bf99-cbd52b83548d/content
6. Таркін В. П. Дезінформація як метод інформаційно-психологічної війни / В. П. Таркін. *Європейський вибір України, розвиток науки та національна безпека в реаліях масштабної військової агресії та глобальних викликів XXI століття* (до 25-річчя Національного університету «Одеська юридична академія» та 175-річчя Одеської школи права) : у 2 т. : матеріали Міжнар.наук.-практ. конф. (м. Одеса, 17 червня 2022 р.) / за загальною редакцією С. В. Ківалова. Одеса : Видавничий дім «Гельветика», 2022. Т. 1. С. 267–270. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/19192/%D0%A2%D0%B0%D1%80%D0%BA%D1%96%D0%BD%20%D0%92%D0%B0%D1%81%D0%B8%D0%BB%D1%8C%20%D0%9F%D0%B0%D0%B2%D0%BB%D0%BE%D0%B2%D0%B8%D1%87.pdf?sequence=1&isAllowed=y
7. Данільян О. Г., Дзьобань О. П., Панов М. І. Національна безпека України: структура та напрямки реалізації : навч. посіб. Харків : Фоліо, 2002. 285 с.
8. Панченко О. Інформаційна складова національної безпеки. *Вісник Національної академії Державної прикордонної служби України.* Випуск 3. 2019. URL: https://periodica.nadpsu.edu.ua/index.php/governance/article/view/296/297

Анотація

У статті проаналізовано сутність та особливості інформаційної війни, враховуючи її міжнародно-правовий контекст. Зазначено, що інформаційна війна є складним явищем, що включає дезінформацію, маніпуляції, кібератаки та інші способи впливу на суспільство з метою досягнення стратегічних цілей. Особлива увага приділена дослідженню впливу інформаційної війни на державний суверенітет, територіальну цілісність та національну безпеку України. Проілюстровано далекосяжні наслідки, які в силу негативного характеру інформаційної війни, мають змогу знищувати довіру громадськості до владних структур, інституцій та засобів масової інформації, а також поширювати ненависть та нетерпимість між національними, етнічними чи релігійними групами.

Автором ретельно розглянуто роль дезінформації як основного інструменту інформаційної війни, його механізми та наслідки для національної безпеки. Досліджено правові аспекти боротьби з дезінформацією та підвищення інформаційної грамотності громадян. Виявляються шляхи, за допомогою яких дезінформаційні кампанії можуть впливати на політичні процеси, соціальну стабільність, економічний розвиток та внутрішню безпеку країни.

Особливу увагу приділено обговоренню ролі державних органів, міжнародних організацій та громадськості у виявленні, запобіганні та протидії інформаційній війні та дезінформації. Враховуючи особливості сучасної політичної картини України та наявність збройного конфлікту, надано рекомендації щодо зміцнення правової бази та механізмів для ефективного протидії інформаційній агресії, прослідженo зв'язок між послабленням національної безпеки країни та зовнішнім інтересом третіх осіб – акторів.

На основі системного аналізу та використання наукової термінології автор робить висновки про необхідність розвитку комплексних заходів та стратегій протидії інформаційним загрозам для збереження національної безпеки України. Акцентується на значущості ролі правового регулювання та створення міжнародних партнерств для спільного протидії інформаційним загрозам і забезпечення сталого розвитку країни.

Ключові слова: інформаційна війна, дезінформація, національна безпека, інформаційна безпека, інформаційна грамотність, безпека, національні інтереси, загрози національній безпеці, система забезпечення національної безпеки, механізми забезпечення національної безпеки.

Kobko Ye. V. Information warfare and disinformation: impact on the National Security of Ukraine

Summary

The article analyzes the essence and features of information warfare, taking into account its international legal context. It is noted that information warfare is a complex phenomenon which includes disinformation, manipulation, cyber attacks and other means of influencing society in order to achieve strategic goals. Particular attention is paid to the study of the impact of information warfare on state sovereignty, territorial integrity and national security of Ukraine. The author illustrates the far-reaching consequences that, due to the negative nature of information warfare, can destroy public trust in government structures, institutions and the media, as well as spread hatred and intolerance between national, ethnic or religious groups.

The author thoroughly examines the role of disinformation as the main tool of information warfare, its mechanisms and consequences for national security. The legal aspects of combating disinformation and raising the information literacy of citizens are studied. The ways in which disinformation campaigns can influence political processes, social stability, economic development and internal security of the country are identified.

Particular attention is paid to discussing the role of government agencies, international organizations and the public in detecting, preventing and countering information warfare and disinformation. Taking into account the peculiarities of the current political picture of Ukraine and the presence of an armed conflict, the author provides recommendations for strengthening the legal framework and mechanisms for effectively countering information aggression, and traces the connection between the weakening of the country's national security and the external interest of third-party actors.

Based on a systematic analysis and the use of scientific terminology, the author draws conclusions about the need to develop comprehensive measures and strategies to counter information threats in order to preserve Ukraine's national security. The author emphasizes the importance of the role of legal regulation and establishment of international partnerships for joint counteraction to information threats and ensuring sustainable development of the country.

Key words: information warfare, disinformation, national security, information security, information literacy, security, national interests, threats to national security, national security system, mechanisms of national security.