Interdisciplinary Studies of Complex Systems
No. 23 (2023) 41–54

https://doi.org/10.31392/iscs.2023.23.041 UDC 316.4:32]:001.102-049.5”364”

Socio-political stability as a component of the information security system: challenges in the context of martial law

Yehor Minenko[1,2], *Kostiantyn Zakharenko*[1,3], *Rostyslav Drapushko*[1,4], *Olha Volianiuko*[1,5]

Суспільно-політична стабільність як складова системи інформаційної безпеки: виклики в умовах воєнного стану

Єгор Міненко, Костянтин Захаренко, Ростислав Драпушко, Ольга Волянюк

Abstract. This article focuses on analyzing the role of information security as a fundamental factor in ensuring political stability and security of citizens, society and the state. In the context of wartime, the emphasis is on identifying and neutralizing the harmful effects of various cyber threats, as well as on strategies to reduce the harmful effects in order to maintain social and political stability. The study notes that Ukraine lacks a comprehensive, effective model for systematically ensuring state, public and individual information security. The authors identify social media, fake or hacked accounts of public figures, as well as local and global messenger chats as the main tools for spreading disinformation in times of war.
Attention is focused on the importance of aspects related to the spread of rumors, gossip, and falsified information in the context of information security. These phenomena are understood to include a wide range of practices, including fake advertising, pseudo-experts, fictitious conspiracies, and manipulative clickbait. Particular attention is paid to the mechanisms of spreading fake news on social media, including the use of bot farms, troll factories, and provocative actions. It is also important to consider fake news as an element of information confrontation in the context of Russian aggression, which involves a clash of different narratives.
Despite numerous scientific works aimed at analyzing the essence of the concept of «information security», studying the main threats to information security, considering the stages of its improvement, the national legal framework for ensuring information security, as well as mechanisms for combating disinformation, no systematic research has been conducted in this area to date that would address the issues of information security in wartime, as well as the main mechanisms for countering disinformation in the context of hostilities.
The purpose of this article is to analyze the challenges and threats to Ukraine's information security in wartime and to identify mechanisms for combating false news under martial law. This research is important for the development of effective information security strategies that take into account the specifics of wartime and the dynamics of geopolitical influences and globalization that Ukraine faces.

[1] Dragomanov Ukrainian State University, Kyiv, Ukraine
[2] y.minenko@smdsu.org.ua, https://orcid.org/0000-0001-7169-3252
[3] Kzakharenko@ukr.net, https://orcid.org/0000-0003-0900-7313
[4] ronadr1502@gmail.com, https://orcid.org/0000-0002-3009-5349
[5] volyanyuk@ukr.net, https://orcid.org/0000-0002-1606-7416

The article describes various components of information security, including information technology and information and psychological protection. Considerable attention is paid to public education in the field of media literacy, dissemination of unadulterated information through state online resources and media, as well as establishing responsibility for the dissemination of fake news. The author also discusses strategies for managing fake accounts and neutralizing fake news, in particular with the help of specialized cyberpolice units. The article also identifies and describes in detail the main directions for improving information security as an important component of Ukraine's national security.

Keywords: information security, hybrid warfare, socio-political stability, countering disinformation, armed aggression

Анотація. Стаття зосереджується на аналізі ролі інформаційної безпеки як фундаментального чинника у забезпеченні політичної стабільності та безпеки громадян, суспільства, держави. У контексті воєнних умов акцент робиться на виявленні та нейтралізації шкідливого впливу різноманітних кіберзагроз, а також на стратегіях зменшення шкідливих наслідків з метою підтримання соціальної та політичної стабільності. У дослідженні відзначено відсутність в Україні комплексної, ефективної моделі для системного забезпечення державної, суспільної та індивідуальної інформаційної безпеки.

В якості основних інструментів поширення дезінформації в умовах війни автори ідентифікують соціальні мережі, підроблені або зламані акаунти публічних особистостей, а також локальні та глобальні чати у месенджерах.

Акцентується увага на значних проблемах, пов'язаних із поширенням чуток, пліток, фальсифікованої інформації у контексті інформаційної безпеки. Під цими феноменами розуміється широкий спектр практик, зокрема фейкова реклама, виступи псевдоекспертів, вигадані змови, маніпулятивні клікбейти. Окрема увага приділяється механізмам поширення фальсифікованих новин у соціальних мережах, наприклад, використанню ботоферм, «фабрик тролів», провокаційних акцій. Важливим є також розгляд фейкових новин як елемента інформаційного протиборства у контексті російської агресії, що передбачає зіткнення різних наративів.

Не зважаючи на численні наукові праці, спрямовані на аналіз сутності поняття «інформаційна безпека», вивчення основних загроз інформаційній безпеці, розгляд етапів її вдосконалення, національних правових основ забезпечення інформаційної безпеки, а також механізмів боротьби з дезінформацією, в цій сфері до сьогоднішнього дня не було проведено системних досліджень, які б розглядали проблематику інформаційної безпеки в умовах воєнного часу, а також основні механізми протидії дезінформації в умовах воєнних дій.

Метою цієї статті є аналіз викликів та загроз інформаційній безпеці України у воєнний час та визначення механізмів боротьби з неправдивими новинами в умовах воєнного стану. Це дослідження має важливе значення для розробки ефективних стратегій інформаційної безпеки, які враховують специфіку воєнного часу та динаміку геополітичних впливів та глобалізації, з якими стикається Україна.

Стаття розкриває різні компоненти інформаційної безпеки, зокрема інформаційні технології та інформаційно-психологічний захист. Значна увага приділяється освіті населення у сфері медіаграмотності, поширенню неспотвореної інформації через державні онлайн-ресурси, медіа, а також встановленню відповідальності за розповсюдження фальсифікованих новин. Окремо обговорюються стратегії управління фейковими акаунтами та нейтралізації фейкових новин, зокрема за допомогою спеціалізованих підрозділів кіберполіції. У статті також визначаються та детально описуються основні напрями вдосконалення інформаційної безпеки як важливої складової національної безпеки України.

Ключові слова: інформаційна безпека, гібридна війна, суспільно-політична стабільність, протидія дезінформації, збройна агресія

Постановка проблеми. У контексті сьогодення, вивчення та аналіз різних теоретичних та концептуальних підходів до поняття «інформаційна безпека» в Україні набуває нової актуальності, що пояснюється наявністю різноманітних, іноді суперечливих, визначень цієї комплексної

та багатогранної категорії. З огляду на багатоаспектність, структурно-функціональний поліморфізм та системну складність категорії, ця стаття прагне систематизувати актуальні підходи до трактування «інформаційної безпеки» [1].

У контексті аналізу останніх досліджень і публікацій, варто відзначити, що автори надають цьому поняттю різних, часом і суперечливих визначень. Наприклад, Т. Ткачук розглядає інформаційну безпеку як комплексну категорію, що охоплює такі аспекти як недосконаліть, несвоєчасність і недостовірність інформації, несанкціоноване поширення та використання інформації, унеможливлення або мінімізація заподіяння шкоди особі, суспільству та державі через негативний вплив інформації або наслідків функціонування інформаційних технологій [2].

Це визначення підкреслює стан захищеності інформаційного простору як ключовий аспект інформаційної безпеки, а також увиразнює поняття «захист національних інтересів України» як основу для обговорення такої тематики.

Можна констатувати, що концепція «інформаційної безпеки» описує широкий спектр заходів та стратегій, спрямованих на протидію шкідливому впливу інформаційних загроз. Ці визначення акцентують на важливості запобігання негативним наслідкам, що можуть виникнути в результаті різних інформаційних викликів, та на розробці ефективних методів ліквідації та управління цими наслідками з мінімальним збитком для суспільства та індивідуальних осіб.

Ключовим аспектом у визначенні інформаційної безпеки є підхід, що розглядає її як системний принцип нормального і безпечного функціонування суспільства в умовах глобального інформаційного простору [3].

В. Гурковський, наприклад, трактує національну інформаційну безпеку України як суспільні відносини, пов'язані зі захистом життєво важливих інтересів людини, громадянина, суспільства та держави від реальних та потенційних загроз в інформаційному просторі [4].

Загалом йдеться про збереження та зміцнення духовних і матеріальних цінностей народу, існування України як суверенної держави, самозбереження та прогресивний розвиток. Таким чином, інформаційна безпека розглядається не тільки як технічна чи оперативна задача, але й як стратегічний елемент національної безпеки, що охоплює широкий спектр соціальних, політичних та культурних вимірів.

Синтезуючи думки українських та зарубіжних дослідників, можна стверджувати, що інформаційна безпека є фундаментальним елементом національної безпеки, що обіймає не лише автономні сфери, але й виступає як інтегральна та всеохоплююча характеристика, яка впливає на громадянську, соціальну та національну безпеку. Цей підхід знаходить широке відображення у теорії та практиці забезпечення національної безпеки, де інформаційна безпека є ключовим компонентом у розробці стратегічних напрямів національної безпеки [3].

У контексті України, наголошується на необхідності постійного оновлення та розвитку науково-теоретичного дискурсу, який би комплексно, структурно та функціонально підходив до вивчення проблеми кібербезпеки. Сучасні умови вимагають ефективної інтеграції цього питання у сферу

забезпечення державної та національної безпеки, де інформаційна безпека розглядається як стан, в якому негативні наслідки використання інформаційних технологій або спеціальних інформаційних операцій не завдають значної шкоди національним інтересам держави.

Значення цієї проблематики зростає у світлі впливу інформаційного тероризму та кіберзлочинності, вимагаючи розробки комплексної теоретичної бази, яка би враховувала філософські, політичні та кібернетичні аспекти. Особливу увагу слід приділити філософсько-аксіологічному аналізу кібербезпеки особистості, в тому числі значимими є філософські, феноменологічні, соціальні та психологічні виміри як особистої, так і суспільної інформаційної безпеки. Концепт «особиста інформаційна безпека» у цьому контексті визначається як захист свідомості та психіки людини від небезпечної інформації, зокрема від маніпуляції свідомістю, дезінформацію, деструктивні впливи тощо.

Таким чином, інформаційна безпека є ключовою складовою інформаційного суспільства та глобальної цивілізації, виконуючи глобальну та інтегровану функцію. Це увиразнює необхідність застосування концептуально-теоретичного принципу системності при розгляді інформаційної безпеки як у національному, так і в міжнародному контексті [3].

Отже, інформаційна безпека осмисллюється як одне з найважливіших понять у різних галузях науки та людської діяльності, відображаючи комплексну природу сучасного інформаційного суспільства.

Аналіз різноманітних підходів до визначення поняття «кібербезпека» виявляє, що жорстке дотримання однієї позиції є недоцільним, особливо в умовах швидкого розвитку інформаційних систем і формування інформаційного суспільства. Таким чином, потрібен гнучкіший, комплексний, системний підхід, що дозволяє врахувати постійну динаміку та розвиток інформаційного сектору. Інтегративний підхід, який об'єднує основні характеристики інформаційної безпеки з урахуванням цієї динаміки, є адекватним цим викликам, розширює розуміння сутності цієї складної системи.

Комплексність проблематики інформаційної безпеки держави, суспільства, людини, дозволяє віднаходити проблеми, що відзначаються особливою актуальністю та потребують перманентного концептуально-теоретичного аналізу, із врахуванням нових інформаційно-технологічних здобутків та динамічних тенденцій і змін на міжнародній арені і в глобальному просторі інформаційної цивілізації [23].

У контексті глобального інформаційного середовища, теоретичні дослідження інформаційної безпеки повинні бути спрямовані на розуміння системного та всеохоплюючого характеру цієї проблематики. Це особливо актуально для України, де, крім забезпечення безпеки державної інформації, виразна потреба в демократизації суспільного життя. Комплекс проблем інформаційної безпеки охоплює широке поле питань, адже йдеться про захист прав і свобод людини у сфері інформації, гарантування національної, культурної та духовної самобутності, а також розвиток національної інформаційної сфери та захист національного інформаційного ринку.

Залучення цих аспектів до дослідження інформаційної безпеки дозволяє ефективніше відповідати на виклики, пов'язані з міжнародною інфор-

маційною безпекою, зокрема запобігати інформаційному тероризму, обмежувати інформаційні потоки в інтересах безпеки та захищати національну інформаційну інфраструктуру. Таким чином, урахування цих векторів діяльності є ключовим для формування ефективної стратегії інформаційної безпеки в Україні.

Роль інформаційної безпеки в процесі державотворення, захисту верховенства права, а також сприянні становленню та розвитку громадянського суспільства в Україні заслуговує на особливу увагу, адже, враховуючи унікальні виклики, з якими стикається держава і суспільство в наш час, важливість розгляду інформаційної безпеки з теоретико-методологічної перспективи стає надзвичайно актуальною. Такий підхід дозволить не тільки краще розуміти виклики, пов'язані з інформаційною безпекою, але й визначити ефективні стратегії для їх подолання.

У цьому зв'язку враховуємо слушні зауваження вчених про те, що органи адміністрування здійснюють свої повноваження відповідно до своїх функцій та приймають національні адміністративні рішення з метою створення правових, організаційних, політичних та економічних умов для реалізації цієї політики на всіх рівнях [22]. Тобто важливо розуміти ширше коло зацікавлених суб'єктів.

Особлива увага в цьому контексті повинна бути приділена вивченню структурно-функціональних характеристик феномену інформаційної безпеки. Важливо визначити конкретні потреби суб'єктів інформаційного забезпечення, які є ключовими в розвитку інформаційного суспільства. Стан інформаційної безпеки суб'єкта досягається через ефективність його діяльності, забезпечену повною, достовірною та достатньою для прийняття рішень інформацією.

Цей стан залежить від трьох основних груп суспільних відносин, що становлять структурні елементи інформаційної безпеки: відносини у сфері інформаційних технологій, відносини, пов'язані з доступом до інформаційних ресурсів, та діяльність у сфері формування цих ресурсів. Перша група забезпечує наявність ефективних засобів для інформаційної діяльності, друга група гарантує доступ до необхідних інформаційних ресурсів, а третя займається формуванням відповідних ресурсів, які відповідають потребам суб'єктів.

Таким чином, інформаційна безпека трактується як комплексна та багатогранна система, що включає різні аспекти інформаційного забезпечення та управління, які є критично важливими для ефективного функціонування держави, суспільства та окремих громадян. Врахування цих аспектів є необхідним для створення міцної та ефективної системи інформаційної безпеки, яка може відповідати сучасним викликам та потребам України.

Визначення концептуальних та теоретичних критеріїв інформаційної безпеки сьогодні є ключовим завданням, яке охоплює різні рівні суспільного функціонування: від національного та регіонального до індивідуального рівня. Такий комплексний підхід необхідний для ефективного реагування на різноманітні виклики, пов'язані з інформаційною безпекою, враховуючи специфічні потреби кожного суб'єкта, від держави до окремої особи.

Одним із важливих орієнтирів у дослідженні інформаційної безпеки в Україні є розробка та оновлення правової бази, яка б відповідала

вимогам сучасного інформаційного суспільства воюючої країни. Існуючі нормативно-правові документи часто є застарілими та не відображають поточних реалій, особливо в контексті швидкого розвитку інформаційних технологій.

Сьогодні існує нагальна потреба у оновленні та розширенні правових рамок інформаційної безпеки для відповідності швидкому розвитку інформаційних технологій і змінам у глобальному інформаційному середовищі.

Ідея застосування високих технологій заради політичного розвитку та модернізації, для оптимізації державних функцій вочевидь користується значною популярністю в українському суспільстві [24].

Ураховуючи важливість розробки нових засад інформаційної безпекової політики в Україні, дослідження інформаційної безпеки в контексті української інформаційної політики, а також порівняльний аналіз цієї політики з практиками провідних країн світу, набуває особливого значення. В умовах глобального інформаційного суспільства, розробка політико-правових інструментів та механізмів захисту інформаційного простору й інформаційної безпеки громадян є важливим викликом, особливо актуальним для України.

Стаття 17 Конституції України визначає інформаційну безпеку як одне з основних завдань держави, поряд із такими аспектами як суверенітет, територіальна цілісність та економічна безпека. Забезпечення інформаційної безпеки передбачається здійснювати через розвиток законодавства, впровадження сучасних і безпечних інформаційних технологій, створення державної інфраструктури, організацію і розвиток інформаційних відносин [7].

Однак, незважаючи на конституційні зобов'язання та прийняття декількох законів у цій сфері, на практиці ці зусилля не відобразилися у значному покращенні стану інформаційної безпеки в країні.

Це свідчить про необхідність подальшого удосконалення правової та політичної бази інформаційної безпеки в Україні у такий спосіб, щоб вона відповідала сучасним вимогам інформаційного суспільства, забезпечувала ефективний захист інформаційного простору країни.

Активний пошук оптимальних законодавчих і нормативно-правових механізмів інформаційної безпеки в Україні, який триває вже багато років, підкреслює важливість цього питання для національної безпеки країни.

Так, Стратегія інформаційної безпеки, затверджена Указом Президента України від 20 грудня 2021 року № 605/2021, визначає інформаційну безпеку України 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 [5].

Проте, Закон України «Про національну безпеку України» відносить інформаційну сферу до області національної безпеки, що не дає чіткого визначення терміну «інформаційна безпека», обмежується лише переліком загроз і напрямів державної політики в цій сфері.

Таким чином, існує необхідність у подальшому вдосконаленні та узгодженні нормативно-правової бази, щоб вона відповідала сучасним вимогам інформаційного суспільства, забезпечувала ефективну політику національної безпеки в інформаційній сфері. Важливо виробити чіткі та послідовні підходи до визначення інформаційної безпеки, щоб вони враховували як технічні, так і ширші соціально-політичні аспекти, а також відповідали реальним потребам і викликам сучасної України.

Відсутність цілісного підходу до інформаційної безпеки в умовах війни, складності розвитку інформаційного суспільства, нові види суспільної комунікації вбачаємо серед основних викликів, з якими стикається Україна. Недостатній рівень інформаційного та аналітичного забезпечення політичного управління ускладнює прийняття виважених рішень та сприяє конфліктам між різними суспільними групами.

Особливу увагу варто приділити розробці комплексного підходу, тобто розвивати правові, технічні, освітні та соціально-комунікаційні стратегії, спрямовані на посилення інформаційної безпеки України. У цьому контексті, Стратегія інформаційної безпеки, затверджена Указом Президента України № 605/2021, відіграє важливу роль, надаючи правову основу для зміцнення інформаційної безпеки та вироблення ефективних механізмів захисту від інформаційних загроз.

Інформаційна безпека в умовах збройної агресії РФ проти України набуває критичного значення. Особливо це стосується викликів, пов'язаних зі спотворенням інформації та активним поширенням дезінформації. Російські медіа репрезентують військове вторгнення як «спеціальну операцію», виправдовуючи агресивні дії, створюючи хибне сприйняття подій.

У цьому контексті інформаційна безпека охоплює не тільки захист від зовнішніх інформаційних загроз, але й підвищення рівня інформаційної грамотності громадян, здатність держави створювати умови для розвитку і задоволення інформаційних потреб особи, а також захист від негативних наслідків неправдивої інформації.

Соціальні мережі та месенджери стають основними каналами поширення дезінформації. Це створює необхідність для вжиття заходів з протидії таким викликам, забезпечуючи надійну інформаційну безпеку в умовах воєнного конфлікту.

Протидія поширенню дезінформації за воєнного стану вимагає комплексного підходу, тобто як технічні рішення (наприклад, фільтрація та моніторинг контенту), так і освітні заходи, спрямовані на підвищення рівня медіаграмотності населення. Це дозволить громадянам критично оцінювати отриману інформацію та відмовлятися від ненадійних джерел новин.

Питання поширення чуток є одним із ключових викликів суспільно-політичній стабільності, оскільки вони можуть мати серйозний вплив на суспільну думку та важливі події, особливо в умовах війни та криз. Чутки, які традиційно були частиною соціальної комунікації, в епоху цифрових технологій набули нових форм.

В умовах війни чутки та дезінформація можуть мати особливо негативний вплив. Наприклад, розповсюдження фейкової інформації про гуманітарну допомогу або військове співробітництво може підривати довіру суспільства до влади, викликати паніку серед населення або навіть завадити проведенню оборонних дій.

Ефективна протидія онлайн-чуткам вимагає комплексного підходу, зокрема:

1) сприяння інформаційній грамотності громадян, розгортання умов для критичного аналізу отриманої інформації;
2) використання технологій моніторингу та фільтрації інформації для виявлення та блокування фейкових новин;
3) активна інформаційна протидія з боку влади та медіа, орієнтація на швидке спростування дезінформації;
4) створення ефективних каналів комунікації між владою, медіа та громадянами для забезпечення швидкого та точного поширення інформації.

Роль уряду та влади є ключовою у формуванні незаангажованого сприйняття подій, у боротьбі з дезінформацією та підтриманні соціальної стабільності, а також довіри громадян.

Інформаційна безпека сьогодні стала центральною темою, особливо у контексті спершу гібридної, а відтак і збройної агресії РФ проти України, розповсюдження державою-агресором неправдивої інформації західними каналами. Поширення чуток та фейкових новин через різноманітні онлайн-платформи та соціальні мережі створює серйозні виклики для інформаційної безпеки. Ці чутки часто позбавленні ґрунтовності, логіки, цілісності, але досить ефективно служать інструментом маніпуляції громадською думкою, впливаючи на перебіг подій та ставлення людей до важливих суспільно-політичних питань.

В умовах глобалізації та розвитку цифрових технологій поширення дезінформації набуло нових масштабів. Швидкість передачі інформації в інтернеті та анонімність користувачів сприяють і динаміці «постправди». Такі новини часто містять непідтверджену інформацію, використовуються для політичної пропаганди, створення негативного іміджу політиків чи дискредитації конкурентів. Це вимагає від громадян бути особливо пильними і критично ставитися до інформації, яку вони споживають.

Ефективна протидія дезінформації та забезпечення інформаційної безпеки вимагають комплексного підходу, зокрема це перевірка джерел інформації, заходи з розвитку критичного мислення, технічні заходи захисту, а також освітні та психологічні стратегії. Важливо, щоб уряди та громадськість активно співпрацювали у боротьбі з фейковими новинами, особливо в умовах військового конфлікту, де дезінформація може мати руйнівний вплив на суспільство та довіру до влади.

Захист від непомітного інформаційного впливу є ключовою частиною інформаційно-психологічної безпеки. Науковці визначають два основні методи такого впливу: навіювання, що діє на несвідомі рівні пам'яті, та зміна свідомості для створення прямого доступу до спогадів. У сучасних військових конфліктах, таких як напад РФ на Україну, фейкові новини та викривлена інформація мають значний вплив на хід подій.

Відтак медіаграмотність стає важливим інструментом протидії дезінформації. Вона розвиває критичне мислення, розуміння медіа, а також навички визначення достовірності інформації. Підвищення медіаграмотності допомагає людям аналізувати інформаційні потоки і захищати себе від маніпулятивного впливу. Особливо це важливо в умовах війни, де інформація часто використовується як засіб психологічного та інформаційного впливу.

Завданням уряду та суспільства є розробка та реалізація ефективних стратегій протидії дезінформації, а це як технічні заходи захисту, так і освітні програми. Вказане дозволить не тільки протистояти поточним викликам, але й зміцнити довгострокову стабільність, безпеку в інформаційному просторі країни.

У сучасних умовах очевидно що інформаційна війна є інтегральною частиною глобального військового конфлікту, а розвиток медіаосвіти, медіаграмотності та зміцнення імунітету суспільства до дезінформації стають важливими аспектами національної безпеки. Очевидно, що РФ докладає значних зусиль для дискредитації українського народу в міжнародному контексті та підриву внутрішньої єдності України. Пропагандистські механізми активно використовуються для розповсюдження проросійських ідеологій та наративів, маючи на меті вплив на свідомість українського населення та використання виявлених в ході війни слабкостей.

Ключовим аспектом протидії дезінформації є світоглядні зміни й аналітичні здібності, що передбачають розуміння мотивів використання певного контенту медіа як інструменту пропаганди та маніпуляцій, а також оцінку цілей недостовірних матеріалів, потенційної шкоди, яку вони можуть завдати. Важливим є усвідомлення масштабу та наслідків шкоди від дезінформації. Другим важливим кроком є об'єктивне висвітлення новин та інформації з боку публічних онлайн-видань та мас-медіа, особливо у воєнні часи, коли постійне та точне інформування може сприяти розвінчуванню міфів та неправдивих чуток.

З початком масштабного вторгнення в Україні на всіх національних телеканалах було запущено спеціальну інформаційну програму під назвою «Єдині новини». Ця програма забезпечує огляд важливих подій, пов'язаних з російським вторгненням, військовими діями, переміщенням ворожих військ і діями української армії. Вона також доповнює випуски аналітикою та коментарями представників уряду, що нерідко засновані на особистих відвідинах фронтових зон. Це сприяє протидії дезінформації, зниженню паніки серед населення, підтримці морального духу, особливо в прифронтових районах.

Висновок. Аналіз сучасного стану інформаційної безпеки в Україні виявляє необхідність зосередження уваги на важливих напрямках її удосконалення. Зокрема, актуальними є стратегічне стримування та припинення воєнних дій, які можуть бути спровоковані через застосування дезінформаційних технологій. Окрім цього, необхідно вдосконалювати системи інформаційної безпеки Збройних Сил України та інших військових формувань, зокрема засоби інформаційної протидії [1]. Ефективне прогнозування, виявлення та оцінка інформаційних загроз, особливо тих, що стосуються збройних сил, є критично важливими. У цьому контексті важливу

роль відіграють органи, відповідальні за забезпечення національної інформаційної безпеки.

Окремо слід зазначити, що інформаційна безпека в Україні має базуватися на координованих діях держави та громадянського суспільства, особливо в умовах війни, де роль інформаційної культури та громадянського спротиву дезінформації значно зростає. В умовах, коли інформація використовується як засіб масового ураження, існує актуальна потреба у створенні ефективних механізмів забезпечення інформаційної безпеки. Такі механізми мають охопити технічні, політичні та правові компоненти: від створення відповідної технічної бази до законодавчого регулювання забезпечення інформаційної безпеки.

Крім того, забезпечення інформаційної безпеки вимагає юридичного регулювання, зокрема введення відповідальності за поширення неправдивої інформації, особливо під час війни.

Враховуючи важливість інформаційної безпеки в умовах воєнних дій, можна констатувати, що дезінформація може викликати значні негативні наслідки, зокрема паніку серед населення, негативний вплив на військову ситуацію, на психологічний стан цивільного населення. План ефективних заходів протидії агресії мав би враховувати не лише внутрішні зусилля, але й активне залучення міжнародних організацій та демократичної спільноти загалом. Перспективи дослідження полягають у вивченні міжнародного досвіду в питаннях протидії дезінформації та висвітленні військових подій у контексті інформаційної війни, що є актуальним за сучасних умов.

Література

[1] Шемчук В. 2020. Конституційно-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз : дис. ... д-ра юрид. наук: 12.00.02. Ужгород. 411 с. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/30707 (дата звернення: 20.11.2023).

[2] Ткачук Т. 2019. Правове забезпечення інформаційної безпеки в умовах євроінтеграції України : дис. ... д-ра юрид. наук : Ужгород, 407 с. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/19617 (дата звернення: 20.11.2023).

[3] Золотар О. О. 2010. Інформаційна безпека людини:теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк». 446 с.

[4] Гурковський В. 2004. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки: дис. ступеня канд. юрид. наук: спец.: 25.00.02 — «Механізми державного управління». Київ. 225 с.

[5] Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України від 20.12.2021 р. № 605/2021. URL: https://zakon.rada.gov.ua/laws/show/605/2021#Text (дата звернення: 19.11.2023).

[6] Про національну безпеку України : Закон України від 21.06.2010 р. № 2469-VIII : станом на 31 берез. 2023 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 19.11.2023).

[7] Конституція України, прийнята на п'ятій сесії Верховної Ради України 20 червня 1996 р. *Відомості Верховної Ради України*. URL: http://zakon2.rada.gov.ua/laws/show/254Рə/96-РўСЃ (дата звернення: 20.11.2023).

[8] Гаврильців М. 2020. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий електронний журнал*. Т. 2. С. 200–203. URL: http://www.lsej.org.ua/2_2020/54.pdf(дата звернення: 20.11.2023).

[9] Довгань О., Ткачук Т. 2010. Система інформаційної безпеки україни: онтологічні виміри. *Інформація і право*. Т. 24, № 1. С. 09–103. URL: https://ippi.org.ua/sites/default/files/11_7.pdf (дата звернення: 20.11.2023).

[10] Інформаційна безпека в умовах війни : прес-дайджест. III кв. 2022 р. / КЗ «ЗОУНБ» ЗОР, Від. наук. інформації та бібліографії ; [підгот. Ю. Щеглова ; ред. Т. Пішванова]. Запоріжжя : [ЗОУНБ], 2022. 24 с. (Український вибір: виклики та перспективи).

[11] Воєнні аспекти протидії «гібридній» агресії: досвід України : монографія. 2020 / колектив авторів ; за заг. ред. А. М. Сиротенка. Київ : НУОУ ім. Івана Черняховського. 176 с.

[12] Національна безпека: моніторинг реалізації законодавства України. 2010. Київ : Інститут законодавства Верховної Ради України. 375 с.

[13] Мороз А. С., Троян С. С. 2022. Безпека інформаційна. *Велика українська енциклопедія*. URL: https://vue.gov.ua/Безпека_інформаційна (дата звернення: 19.11.2023).

[14] Захаренко К. 2015. Держава як суб'єкт інформаційної безпеки суспільства. *Політологічний вісник*. Вип. 70. С. 06–96.

[15] Захаренко К. 2010. Теоретичні засади дослідження інформаційної безпеки. *Міжнародні відносини, суспільні комунікації та регіональні студії*. № 2 (4). С. 107–116.

[16] Золотар О. О. 2014. Загрози інформаційній безпеці людини. Правова інформатика. № 2 (42). С. 70–79.

[17] Захаренко К. 2010. Категорія інформаційної безпеки у вітчизняному філософсько-політологічному дискурсі. *Вища освіта України*. № 1 (60). С. 40–54.

[18] Міненко Є. С. 2022. Основні засади формування та реалізації державної політики інформаційної безпеки в умовах вітчизняної війни. *Публічне управління та адміністрування в умовах війни і в поствоєнний період в Україні* : матеріали Всеукр. наук.-практ. конф. у трьох томах, м. Київ, ДЗВО «Університет менеджменту освіти» НАПН України, 15–20 квітня 2022 р.; ред. колегія : І. О. Дегтярьова, В. С. Куйбіда, П. М. Петровський та ін., уклад. Т. О. Мельник. Т. 1. Київ : ДЗВО «УМО» НАПН України. 213 с.

[19] Міненко Є. С. 2022. Вплив сучасних інформаційних технологій на психологічний стан особистості. *The 4 th International scientific and practical conference — Modern research in world science* (July 10-12, 2022) SPC, Sci-conf.com.ua, Lviv, Ukraine. 1161 p. URL: https://sci-conf.com.ua/wp-content/uploads/2022/07/MODERN-RESEARCH-IN-WORLD-SCIENCE-10-12.07.22.pdf (дата звернення: 20.11.2023)

[20] Міненко Є. С. 2021. Основні засади формування та реалізації державної політики інформаційної безпеки. *Міжнародна наукова інтернет-*

конференція «Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення» : збірник тез доповідей. Вип. 55 (м. Тернопіль, 9 лютого 2021 р.). Тернопіль. 90 с.

[21] Мазуренко Л. І. 2022. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна*. Серія «Питання політології». Вип. 42. С. 50–57. https://doi.org/10.26565/2220-0009-2022-42-00.

[22] Драпушко Р., Горінов П., Міненко Є. 2022. Ефективність залучення молоді до прийняття управлінських рішень. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* Серія: Публічне управління та адміністрування. Том 33(72). № 3. С. 54–59.

[23] Захаренко К. В. 2021. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : дис. ... д-ра політ. наук : 23.00.02. Київ. 423 с. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf(дата звернення: 20.11.2023).

[24] Волянюк О. 2019. Політична реальність і доповнена реальність: особливості сумісності. *Науковий часопис Національного педагогічного університету імені М. П. Драгоманова*. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін : збірник наукових праць. / [Відп. ред. О. В. Бабкіна]. Вип. 26. С. 06-93.

References

[1] Shemchuk V. 2020. Konstytutsiino-pravove zabezpechennia informatsiinoi bezpeky suchasnykh derzhav: porivnialno-pravovyi analiz : dys. ... d-ra yuryd. nauk : 12.00.02. Uzhhorod. 411 s. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/30707 (data zvernennia: 20.11.2023).

[2] Tkachuk T. 2019. Pravove zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy : dys. ... d-ra yuryd. nauk : Uzhhorod. 407 s. URL: https://www.uzhnu.edu.ua/uk/infocentre/get/19617 (data zvernennia: 20.11.2023).

[3] Zolotar O. O. 2010. Informatsiina bezpeka liudyny:teoriia i praktyka : monohrafiia. Kyiv : TOV «Vydavnychyi dim «ArtEk». 446 s.

[4] Hurkovskyi V. 2004. Orhanizatsiino-pravovi pytannia vzaiemodii orhaniv derzhavnoi vlady u sferi natsionalnoi informatsiinoi bezpeky: dys. stupenia kand. yuryd. nauk: spets. : 25.00.02 «Mekhanizmy derzhavnoho upravlinnia». Kyiv. 225 s.

[5] Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky» : Ukaz Prezydenta Ukrainy vid 20.12.2021 r. № 605/2021. URL: https://zakon.rada.gov.ua/laws/show/605/2021#Text (data zvernennia: 19.11.2023).

[6] Pro natsionalnu bezpeku Ukrainy : Zakon Ukrainy vid 21.06.2010 r. № 2469-VIII : stanom na 31 berez. 2023 r. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (data zvernennia: 19.11.2023).

[7] Konstytutsiia Ukrainy, pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 20 chervnia 1996 r. *Vidomosti Verkhovnoi Rady Ukrainy*. URL: http://zakon2.rada.gov.ua/laws/show/254Рə/96-РўСЃ (data zvernennia: 20.11.2023).

[8] Havryltsiv M. 2020. Informatsiina bezpeka derzhavy v systemi natsionalnoi

bezpeky Ukrainy. *Yurydychnyi naukovyi elektronnyi zhurnal.* T. 2. S. 200–203. URL: http://www.lsej.org.ua/2_2020/54.pdf (data zvernennia: 20.11.2023).

[9] Dovhan O., Tkachuk T. 2010. Systema informatsiinoi bezpeky ukrainy: ontolohichni vymiry. *Informatsiia i pravo.* T. 24, № 1. S. 09–103. URL: https://ippi.org.ua/sites/default/files/11_7.pdf (data zvernennia: 20.11.2023).

[10] Informatsiina bezpeka v umovakh viiny : pres-daidzhest. III kv. 2022 r. / KZ «ZOUNB» ZOR, Vid. nauk. informatsii ta bibliohrafii ; [pidhot. Yu. Shchehlova ; red. T. Pishvanova]. Zaporizhzhia : [ZOUNB], 2022. 24 s. (Ukrainskyi vybir: vyklyky ta perspektyvy).

[11] Voienni aspekty protydii «hibrydnii» ahresii: dosvid Ukrainy : monohrafiia. 2020. / kolektyv avtoriv ; za zah. red. A. M. Syrotenka. Kyiv : NUOU im. Ivana Cherniakhovskoho, 176 s.

[12] Natsionalna bezpeka: monitorynh realizatsii zakonodavstva Ukrainy. 2010. Kyiv : Instytut zakonodavstva Verkhovnoi Rady Ukrainy. 375 s.

[13] Moroz A. S., Troian S. S. 2022. Bezpeka informatsiina. *Velyka ukrainska entsyklopediia.* URL: https://vue.gov.ua/Безпека_інформаційна. (data zvernennia: 19.11.2023).

[14] Zakharenko K. 2015. Derzhava yak sub'iekt informatsiinoi bezpeky suspilstva. *Politolohichnyi visnyk.* Vyp. 70. S. 06–96.

[15] Zakharenko K. 2010. Teoretychni zasady doslidzhennia informatsiinoi bezpeky. *Mizhnarodni vidnosyny, suspilni komunikatsii ta rehionalni studii.* № 2 (4). S. 107–116.

[16] Zolotar O. O. 2014. Zahrozy informatsiinii bezpetsi liudyny. *Pravova informatyka.* № 2 (42). S. 70–79.

[17] Zakharenko K. 2010. Katehoriia informatsiinoi bezpeky u vitchyznianomu filosofsko-politolohichnomu dyskursi. *Vyshcha osvita Ukrainy.* № 1 (60). S. 40–54.

[18] Minenko Y. S. 2022. Osnovni zasady formuvannia ta realizatsii derzhavnoi polityky informatsiinoi bezpeky v umovakh vitchyznianoi viiny. *Publichne upravlinnia ta administruvannia v umovakh viiny i v postvoiennyi period v Ukraini* : materialy Vseukr. nauk.-prakt. konf. u trokh tomakh, m. Kyiv, DZVO «Universytet menedzhmentu osvity» NAPN Ukrainy, 15–20 kvitnia 2022 r.; red. kolehiia : I. O. Dehtiarova, V. S. Kuibida, P. M. Petrovskyi ta in., uklad. T. O. Melnyk. T. 1. K. : DZVO «UMO» NAPN Ukrainy. 213 s.

[19] Minenko Y. S. 2022. Vplyv suchasnykh informatsiinykh tekhnolohii na psykholohichnyi stan osobystosti. *The 4 th International scientific and practical conference —Modern research in world science*‖ (July 10-12, 2022) SPC —Sci-conf.com.ua‖, Lviv, Ukraine. 1161 p. URL: https://sci-conf.com.ua/wp-content/uploads/2022/07/MODERN-RESEARCH-IN-WORLD-SCIENCE-10-12.07.22.pdf (data zvernennia: 20.11.2023)

[20] Minenko Y. S. 2021. Osnovni zasady formuvannia ta realizatsii derzhavnoi polityky informatsiinoi bezpeky. *Mizhnarodna naukova internet-konferentsiia «Informatsiine suspilstvo: tekhnolohichni, ekonomichni ta tekhnichni aspekty stanovlennia»* : zbirnyk tez dopovidei. Vyp. 55 (m. Ternopil, 9 liutoho 2021 r.). Ternopil. 90 s.

[21] Mazurenko L. I. 2022. Informatsiina bezpeka v umovakh rosiisko-ukrainskoi viiny: vyklyky ta zahrozy. *Visnyk Kharkivskoho natsionalnoho universytetu imeni V. N. Karazina.* Seriia «Pytannia politolohii». Vyp. 42. S. 50-57. https://doi.org/10.26565/2220-0009-2022-42-00.

[22] Drapushko R., Horinov P., Minenko Y. 2022. Efektyvnist zaluchennia molodi do pryiniattia upravlinskykh rishen. *Vcheni zapysky Tavriiskoho natsionalnoho universytetu imeni V. I. Vernadskoho*. Seriia: Publichne upravlinnia ta administruvannia. Tom 33(72) № 3. S. 54–59.

[23] Zakharenko K. V. 2021. Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy: transformatsiini vyklyky, hlobalni konteksty, stratehichni oriientyry : dys. ... d-ra polit. nauk : 23.00.02. Kyiv, 423 s. URL: https://lnu.edu.ua/wp-content/uploads/2021/04/dis_zakharenko.pdf (data zvernennia: 20.11.2023).

[24] Volianiuk O. 2019. Politychna realnist i dopovnena realnist: osoblyvosti sumisnosti. *Naukovyi chasopys Natsionalnoho pedahohichnoho universytetu imeni M. P. Drahomanova*. Seriia 22. Politychni nauky ta metodyka vykladannia sotsialno-politychnykh dystsyplin : zbirnyk naukovykh prats / [Vidp. red. O. V.Babkina]. Vyp. 26. S. 06–93.