DOI 10.52363/2414-5866-2025-2-12
УДК 351.746:004.056(477)

Палюх В. В. *д.держ.упр., с.д., НУЦЗУ, м. Черкаси,*
ORCID: 0000-0001-9429-2013,
Новак В.М., *аспірант НУЦЗУ, м. Черкаси,*
ORCID: 0009-0003-6516-0742

Paliukh V., *Doctor of Sciences in Public Administration, Senior Researcher, Head of Doctoral and Adjunct Studies, National University of Civil Defence of Ukraine, Cherkasy,*
Novak V., *Master of Public Administration, PhD student at the National University of Civil Defence of Ukraine*

ВРАЗЛИВОСТІ ІНФОРМАЦІЙНИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНИХ ЗАГРОЗ: МЕХАНІЗМИ ДЕРЖАВНОЇ ПРОТИДІЇ

VULNERABILITIES OF INFORMATION COMMUNICATIONS UNDER HYBRID THREATS: STATE COUNTERACTION MECHANISMS

Проаналізовано вразливості сучасних інформаційних комунікацій в умовах гібридних загроз національній безпеці України. Досліджено особлтивості трансформації інформаційного суспільства у напрямку «інформаціонального» суспільства за М. Кастельсом, що характеризується домінуванням мережевих комунікацій та масових самокомунікацій. Розкрито амбівалентний характер сучасних мережевих технологій, які одночасно створюють нові можливості для демократичної участі громадян та породжують серйозні уразливості для національної безпеки. Особливу увагу приділено аналізу ризиків, пов'язаних з поширенням дезінформації, маніпулятивними впливами через соціальні мережі, фрагментацією інформаційного простору та зниженням ролі традиційних ЗМІ. Обґрунтовано необхідність формування комплексної системи державного управління протидією інформаційним загрозам, що поєднує правове регулювання, технологічні рішення, медіаграмотність населення та міжнародну співпрацю. Запропоновано механізми підвищення стійкості інформаційної інфраструктури України в умовах російської агресії та гібридної війни.

Ключові слова: *інформаційні комунікації, гібридні загрози, державне управління, національна безпека, мережеві технології, дезінформація, кібербезпека, медіаграмотність.*

The article examines the vulnerabilities of modern information communications under hybrid threats to Ukraine's national security. The transformation of information

ISSN 2414-5858 (Print)
ISSN 2414-5866 (Online)

society towards 'informational' society according to M. Castells is analyzed, characterized by the dominance of network communications and mass self-communications. The ambivalent nature of modern network technologies is revealed, which simultaneously create new opportunities for democratic citizen participation and generate serious vulnerabilities for national security. Special attention is paid to analyzing risks related to disinformation spread, manipulative influences through social networks, information space fragmentation, and declining role of traditional media. The necessity of forming a comprehensive public administration system for countering information threats is substantiated, combining legal regulation, technological solutions, population media literacy, and international cooperation. Mechanisms for increasing Ukraine's information infrastructure resilience under Russian aggression and hybrid warfare conditions are proposed.

Keywords: *information communications, hybrid threats, public administration, national security, network technologies, disinformation, cybersecurity, media literacy.*

Постановка проблеми. Сучасний етап розвитку української держави характеризується безпрецедентними викликами у сфері інформаційної безпеки, зумовленими російською збройною агресією та широкомасштабною гібридною війною. В умовах 2025 року, коли Україна продовжує відстоювати свою незалежність та територіальну цілісність, питання захисту інформаційного простору набуває критичного значення для національної безпеки. Трансформація глобального інформаційного середовища, перехід від традиційних форм масової комунікації до мережевих технологій та масових самокомунікацій створили принципово нові уразливості, якими активно користуються ворожі актори для дестабілізації українського суспільства.

Розвиток інформаціонального суспільства в Україні відбувається в умовах постійного інформаційного тиску з боку російської федерації, яка використовує весь спектр гібридних методів впливу – від класичної пропаганди до складних кібератак та маніпуляцій у соціальних мережах. Особливої актуальності набуває проблема протидії дезінформації, яка поширюється через цифрові платформи зі швидкістю, що перевищує можливості традиційних механізмів верифікації та спростування. Амбівалентний характер сучасних комунікаційних технологій проявляється в тому, що ті самі інструменти, які забезпечують демократичну участь громадян та свободу слова, можуть бути використані для підриву демократичних інститутів та національної єдності.

Аналіз останніх вітчизняних і зарубіжних досліджень. Проблематика уразливостей інформаційних комунікацій в умовах гібридних загроз активно досліджується як вітчизняними, так і зарубіжними науковцями. Серед українських дослідників варто відзначити праці О.В. Бантишева, Г.П. Ситника, В.П. Горбуліна, які розглядають питання інформаційної безпеки в контексті національної безпеки України. Особливу увагу заслуговують ро-

боти О.С. Власюка, С.А. Пирожкова, які аналізують механізми протидії гібридним загрозам в умовах російської агресії.

Теоретичні засади дослідження інформаціонального суспільства закладено в роботах М. Кастельса, який ввів поняття "простору потоків" та "масових самокомунікацій". Значний внесок у розуміння амбівалентності сучасних комунікаційних технологій зробили З. Бауман, Н. Луман, які досліджували системні уразливості складних соціальних систем. Проблеми цифрової трансформації державного управління та кібербезпеки розглядаються в працях В.М. Фурашева, О.В. Кузьменка, А.І. Семенченка.

У зарубіжній науковій літературі питання протидії інформаційним загрозам досліджуються в роботах Т. Рід (T. Rid), А. Лукаса (A. Lucas), Дж. Ная (J. Nye), які аналізують еволюцію концепції "гібридної війни" та її інформаційного компонента. Механізми державної протидії дезінформації розглядаються в дослідженнях Європейського центру передового досвіду з протидії гібридним загрозам (Hybrid CoE) та Інституту стратегічного діалогу (ISD).

Попри значний науковий доробок у цій сфері, залишаються недостатньо дослідженими питання системного аналізу уразливостей сучасних інформаційних комунікацій в умовах гібридних загроз, а також розроблення комплексних механізмів державної протидії цим викликам з урахуванням специфіки української моделі державного управління.

Постановка завдання. Метою статті є аналіз основних уразливостей сучасних інформаційних комунікацій в умовах гібридних загроз та розроблення рекомендацій щодо вдосконалення механізмів державної протидії інформаційним атакам в Україні.

Виклад основного матеріалу дослідження. Трансформація інформаційного простору в умовах цифрової революції призвела до формування якісно нового типу суспільства, яке характеризується як "інформаціональне". На відміну від класичного "інформаційного суспільства", в інформаціональному суспільстві знання та інформація стають найпотужнішими ресурсами, що поширюються через мережеві комунікації та здійснюють фундаментальний вплив на всі сфери суспільного життя [3].

Ключовою характеристикою інформаціонального суспільства є мережева логіка його базової структури. Інформаційні мережі по-новому організовують виробництво, управління та комунікацію в глобальному масштабі, що призводить до зменшення ролі національних держав, оскільки їхні кордони перестають бути перешкодою на шляху інформаційних потоків. В Україні ця тенденція проявляється особливо гостро в умовах гібридної війни, коли ворожі інформаційні впливи легко перетинають державні кордони через цифрові канали [1]. Аналіз сучасного стану інформаційних комунікацій в Україні дозволяє виділити кілька критичних уразливостей, які можуть бути використані в межах гібридних загроз. По-перше, фрагментація інфор-

маційного простору внаслідок розвитку соціальних мереж та алгоритмів персоналізації контенту призводить до створення "інформаційних бульбашок", де користувачі отримують лише ту інформацію, яка підтверджує їхні наявні переконання. Це створює сприятливе середовище для поширення дезінформації та радикалізації поглядів [4].

По-друге, спостерігається зниження ролі традиційних ЗМІ як головних джерел достовірної інформації. Традиційні засоби масової інформації втрачають свою роль, поступаючись місцем неформальним джерелам у соціальних мережах. Це ускладнює контроль якості інформації та створює можливості для маніпуляцій. Сучасні цифрові платформи дозволяють миттєво поширювати інформацію серед мільйонів користувачів, що значно перевищує швидкість механізмів верифікації та спростування [5].

По-третє, розвиток штучного інтелекту та ботів дозволяє автоматизувати процеси створення та поширення контенту, що ускладнює ідентифікацію джерел інформації та робить можливими масштабні координовані атаки. Особливої уваги потребує проблема "діпфейків" – синтетичних медіаматеріалів, створених за допомогою штучного інтелекту, які можуть бути використані для дискредитації публічних осіб та дестабілізації суспільства [6].

По-четверте, швидкий розвиток цифрових технологій випереджає адаптаційні можливості користувачів, що робить їх уразливими до маніпулятивних впливів та дезінформації. Зниження медіаграмотності населення, особливо серед старшого покоління, створює додаткові ризики для інформаційної безпеки держави [2].

Формування ефективної системи протидії інформаційним загрозам в Україні потребує комплексного підходу, що поєднує правові, технологічні, освітні та організаційні заходи. Система державного управління у цій сфері має базуватися на принципах пропорційності, прозорості та дотримання демократичних цінностей. Правове регулювання включає вдосконалення законодавства про інформаційну безпеку, регулювання діяльності соціальних мереж та встановлення відповідальності за поширення дезінформації. Ключову роль відіграють Верховна Рада України, РНБО та спеціалізовані регуляторні органи. Технологічний захист передбачає створення систем виявлення дезінформації, забезпечення кібербезпеки критичної інфраструктури та блокування шкідливого контенту. Відповідальними органами є Державна служба спеціального зв'язку, СБУ та Міністерство цифрової трансформації [7].

Медіаграмотність населення забезпечується через освітні програми з медіаграмотності, підготовку державних службовців та інформаційні кампанії для населення. Координацію здійснюють Міністерство освіти і науки, НАДС та громадські організації. Міжнародна співпраця включає обмін досвідом з країнами ЄС та НАТО, участь у міжнародних ініціативах з протидії дезінформації та розвиток спільних технологічних рішень [4].

Особливої уваги потребує розроблення стратегії протидії маніпулятивним впливам через соціальні мережі. В умовах 2025 року, коли близько 75% населення України активно користується соціальними мережами, ці платформи стали основним полем битви за інформаційний простір. Російські спецслужби активно використовують боти, тролі та координовані неавтентичні кампанії для поширення дезінформації та розпалювання внутрішніх конфліктів в українському суспільстві [1].

Перспективним напрямом є розвиток технологій штучного інтелекту для автоматичного виявлення дезінформації та координованих інформаційних атак. Такі системи, інтегровані з моніторингом соціальних мереж та традиційних ЗМІ, дозволять значно підвищити швидкість реагування на інформаційні загрози та зменшити їхній потенційний вплив на суспільство. Важливим є створення Національного центру протидії дезінформації при РНБО України, який координуватиме діяльність усіх державних органів у цій сфері [3].

Висновки. Проведене дослідження дозволяє сформулювати такі висновки:

По-перше, трансформація інформаційного простору в напрямку інформаціонального суспільства створила принципово нові уразливості, які активно експлуатуються в межах гібридних загроз національній безпеці України. Амбівалентний характер сучасних комунікаційних технологій потребує збалансованого підходу до їхнього регулювання, що не обмежуватиме демократичні свободи, але забезпечуватиме захист від ворожих впливів.

По-друге, ефективна протидія інформаційним загрозам потребує комплексного підходу, що поєднує правові, технологічні, освітні та організаційні заходи. Ключову роль відіграє підвищення медіаграмотності населення та формування критичного мислення, особливо серед молоді, яка є найбільш активною у використанні цифрових технологій.

По-третє, система державного управління протидією інформаційним загрозам має базуватися на принципах прозорості, підзвітності та дотримання демократичних цінностей. Надмірне обмеження інформаційних свобод може призвести до зворотного ефекту та підірвати довіру громадян до державних інститутів.

Перспективи подальших досліджень пов'язані з розробленням конкретних методик оцінки ефективності заходів протидії дезінформації, аналізом впливу штучного інтелекту на трансформацію інформаційного простору, а також вивченням можливостей міжнародної співпраці у сфері протидії гібридним загрозам в умовах глобалізації інформаційних процесів.

Список використаних джерел:

1. Закон України "Про інформацію" від 2 жовтня 1992 року № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
2. Закон України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
3. Закон України "Про Раду національної безпеки і оборони України" від 5 березня 1998 року № 183/98-ВР. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр.
4. Закон України "Про телебачення і радіомовлення" від 21 грудня 1993 року № 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12.
5. Стратегія інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 року № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017.
6. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021.
7. Стратегія національної безпеки України, затверджена Указом Президента України від 14 вересня 2020 року № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020.

References:

1. Law of Ukraine "On Information" dated October 2, 1992 No. 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12.
2. Law of Ukraine "On National Security of Ukraine" dated June 21, 2018 No. 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19.
3. Law of Ukraine "On the National Security and Defense Council of Ukraine" dated March 5, 1998 No. 183/98-VR. URL: https://zakon.rada.gov.ua/laws/show/183/98-вр.
4. Law of Ukraine "On Television and Radio Broadcasting" dated December 21, 1993 No. 3759-XII. URL: https://zakon.rada.gov.ua/laws/show/3759-12.
5. Information Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated February 25, 2017 No. 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017.
6. Cybersecurity Strategy of Ukraine, approved by the Decree of the President of Ukraine dated August 26, 2021 No. 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021
7. National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated September 14, 2020 No. 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020.

дата надходження статті: 25.10.2025
дата прийняття статті: 26.11.2025
дата публікації: 27.12.2025