УДК 351.746:004]:167.1-048.23(477)
DOI: https://doi.org/10.31470/2786-6246-2023-3-59-65

Вячеслав РЕДЗЮК,
кандидат історичних наук, доцент, доцент кафедри публічного управління та адміністрування, декан факультету гуманітарно-природничої освіти і соціальних технологій Університету Григорія Сковороди в Переяславі

Vyacheslav REDZIUK,
PhD in History, Associate Professor, Associate Professor of Public Administration and Management, Dean of the Faculty of Humanities and Natural Sciences Education and Social Technologies of Hryhorii Skovoroda University in Pereiaslav

ORCID: https://orcid.org/0000-0003-1762-5042
redziuk@ukr.net

Наталія РЕДЗЮК,
викладачка кафедри публічного управління та адміністрування, аспірантка Університету Григорія Сковороди в Переяславі

Natalia REDZIUK,
Lecturer at the Department of Public Management and Administration, Postgraduate student of Hryhorii Skovoroda University in Pereiaslav

ORCID: http://orcid.org/0000-0002-8697-349X
natatkachuk473@gmail.com

СУЧАСНІ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ТА НАПРЯМИ ЇХ ВИРІШЕННЯ

MODERN PROBLEMS OF INFORMATION SECURITY OF UKRAINE AND DIRECTIONS OF THEIR SOLUTION

Анотація. *У статті розглянуто актуальні проблеми інформаційної безпеки в Україні та запропоновані напрями їх вирішення, адже висхідна роль технологій та інформаційних мереж у сучасному суспільстві ставить перед Україною складні завдання щодо забезпечення конфіденційності, цілісності та доступності інформації. Актуальність теми визначається загрозами кібератак, дестабілізацією інформаційного простору та важливістю забезпечення належного функціонування державних та громадських інформаційних систем. У статті аналізуються сучасні виклики, пов'язані з кіберзагрозами, дезінформацією та кібератаками на критичну інфраструктуру. Запропоновані напрями розв'язання проблем базуються на створенні ефективних механізмів кіберзахисту, підвищенні кіберграмотності населення та розвитку співпраці між державними органами, приватним сектором та міжнародними партнерами. У статті вказано, що на сьогодні однією з основних проблем, які виникають у контексті забезпечення інформаційної безпеки в Україні, є прояв інформаційної експансії та недостатньо об'єктивне та неупереджене відображення подій та ситуацій, що походять від Російської Федерації. Держава-агресор застосовує гібридні технології, включаючи методи інформаційного втручання, задля дестабілізації національної безпеки України. Ми зазначили на необхідності системного підходу до забезпечення інформаційної безпеки та активної ролі держави у розробці та*

впровадженні стратегічних заходів у цій сфері. Державна політика інформаційної безпеки важлива для національної безпеки та має базуватися на системній передбачливій діяльності органів державного управління, що забезпечує гарантії інформаційної безпеки для осіб, соціальних груп, суспільства та держави загалом. Дослідження інформаційної безпеки як об'єкта злочинів проти основ національної безпеки України в умовах війни має велике значення та є надзвичайно актуальним.

Ключові слова: *інформаційна безпека, інформаційний простір, національна безпека, дезінформація, кібератаки, кіберзахист, цифрова грамотність.*

Abstract. *The article discusses the current problems of information security in Ukraine and suggests ways to solve them, since the growing role of technology and information networks in modern society poses complex challenges to Ukraine in terms of ensuring the confidentiality, integrity and availability of information. The relevance of the topic is determined by the threats of cyberattacks, destabilization of the information space and the importance of ensuring the proper functioning of state and public information systems. The article analyzes current challenges related to cyber threats, disinformation and cyber attacks on critical infrastructure. The proposed solutions are based on the creation of effective cyber defense mechanisms, raising cyber literacy of the population, and developing cooperation between government agencies, the private sector, and international partners. The article indicates that today one of the main problems that arise in the context of ensuring information security in Ukraine is the manifestation of information expansion and insufficiently objective and impartial reflection of events and situations originating from the Russian Federation. The aggressor state uses hybrid technologies, including methods of information interference, to destabilize the national security of Ukraine. We have emphasized the need for a systematic approach to information security and the active role of the state in the development and implementation of strategic measures in this area. The State policy of information security is important for national security and should be based on systematic and prudent activities of public administration bodies, which provides guarantees of information security for individuals, social groups, society and the State as a whole. The study of information security as an object of crimes against the foundations of Ukraine's national security in times of war is of great importance and is extremely relevant.*

Key words: *information security, information space, national security, disinformation, cyberattacks, cyber defense, digital literacy.*

Постановка проблеми. Сучасний світ характеризується швидким розвитком інформаційних технологій, що відкриває безмежні можливості для зв'язку, обміну знаннями та доступу до інформації. Проте, разом з цим, збільшується і ризик надмірної вразливості перед інформаційними загрозами та кібератаками. Україна не залишається поза цими процесами, зокрема має низку сучасних проблем інформаційної безпеки, які ставлять під загрозу національну безпеку та суверенітет. Однією з ключових проблем є активна інформаційна експансія з боку Російської Федерації, яка спрямована на дезінформацію, маніпуляцію громадською думкою та дестабілізацію суспільно-політичної ситуації в Україні. Це призводить до необ'єктивного та спотвореного висвітлення фактів і подій, впливає на суспільний дискурс та внутрішню стабільність країни. Важливою проблемою є зростання кількості кібератак на інформаційну інфраструктуру України, що загрожує конфіденційності, цілісності та доступності важливих даних та інформаційних систем. Це має негативний вплив на фінансову, економічну та політичну стабільність країни.

Враховуючи ці проблеми, важливо розглянути напрями розв'язання проблем інформаційної безпеки, включаючи розробку ефективної системи протидії дезінформації,

посилення кібербезпеки, підвищення цифрової грамотності населення та зміцнення співпраці між різними суб'єктами для забезпечення стійкості інформаційного простору України.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки України аналізують вітчизняні та закордонні вчені в різних галузях науки, у тому числі правознавці, політологи, соціологи, психологи, державні управлінці. Зокрема, інформаційну безпеку України аналізують такі вчені, як В. Антонов, В. Бондаренко, В. Бурячок, П. Гаранюк, Ю. Горбань, В. Демиденко, М. Дмитренко, О. Зозуля, О. Когут, А. Крупнова, Р. Кукляк, Ю. Лісовська, Ф. Медвідь, Я. Михальський, А. Нашинець-Наумова, О. Панченко, А. Пишна, А. Платоненко, Д. Пушман, І. Сопілко, А. Сулайман, Ю. Ткач, В. Толубко, В. Фурашева, О. Черевко, Я. Чмир, Д. Шац та ін.

Метою статті є критичний аналіз особливостей інформаційної безпеки України та напрями їх вирішення.

Виклад матеріалу. Інформаційна безпека – це комплекс заходів, стратегій та політик, спрямованих на забезпечення захисту інформаційних ресурсів, даних та інфраструктури від загроз, які можуть призвести до несанкціонованого доступу, втрати, пошкодження чи некоректного використання інформації. Інформаційна безпека також охоплює заходи щодо забезпечення конфіденційності, цілісності та доступності інформації, зокрема запобігання кібератакам, витокам даних та іншим загрозам, які можуть спричинити серйозні наслідки для організацій, держав та особистостей [3].

Обсяг проблем, пов'язаних з використанням інформаційних систем, можна розділити на такі категорії: забезпечення доступності, цілісності та конфіденційності інформаційних ресурсів і супутньої інфраструктури. Інформаційна безпека не зводиться лише до захисту від несанкціонованого доступу до інформації, але являє собою широке та комплексне поняття [1].

В умовах повномасштабного вторгнення Російської Федерації в Україну питання про необхідність єдиної інформаційної політики стало ще більш актуальним. Враховуючи вказане Президентом України був підписав Указ № 152/2022, яким уведено в дію Рішення Ради Національної Безпеки і Оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» [5]. Рішення наголошує на тому, що в умовах воєнного стану інформаційна політика стає однією з ключових складових національної безпеки. Воєнний стан призводить до підвищення загроз інформаційної безпеки, зокрема через можливість посилення дезінформації, пропаганди, кібератак та інших загроз в інформаційній сфері.

Рішення Ради Національної безпеки і оборони України визначає основні напрямки реалізації єдиної інформаційної політики в умовах воєнного стану, а саме:

- забезпечення доступу до об'єктивної інформації, та підкреслює важливе значення надання громадянам вірогідної та об'єктивної інформації про ситуацію на фронті та в країні загалом. Це допомагає запобігти поширенню дезінформації та паніки;
- контроль інформаційного простору, що визначає потребу у підсиленні заходів для контролю та координації інформаційного простору в умовах воєнного стану. Це може включати запобігання поширенню неперевіреної інформації та пропаганди, а також впливу на соціальні мережі та медіа;
- захист інформаційної інфраструктури вказує на необхідність підвищення рівня кібербезпеки та захисту інформаційної інфраструктури країни в умовах воєнного стану;
- реагування на інформаційні загрози акцентує на важливості оперативного та ефективного реагування на інформаційні загрози, включаючи кібератаки, дезінформацію та інші загрози для національної безпеки;

- співпраця з міжнародним співтовариством, адже рішення визначає потребу у зміцненні співпраці з міжнародними партнерами у сфері інформаційної безпеки, обміну досвідом та ресурсами для ефективної протидії загрозам.

Ми вважаємо, що хоч Рішення Ради Національної Безпеки і Оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» має важливу роль у забезпеченні інформаційної безпеки країни, в ньому також можна виділити деякі негативні аспекти, а саме:

- потенційну обмеженість свободи інформації, адже в умовах воєнного стану, під виглядом захисту національної безпеки, можуть виникнути ситуації, коли може бути обмежено розповсюдження певних інформаційних матеріалів або поглядів, що порушує свободу слова та доступ до інформації;
- можливість маніпуляцій, адже під час реалізації єдиної інформаційної політики є ризик маніпулювання інформацією для політичних чи стратегічних цілей, що може призвести до недостатньо об'єктивного висвітлення подій та створення спотворених перспектив;
- потенційну нерівновагу в доступі до інформації, адже при здійсненні інформаційних заходів в умовах воєнного стану виникає обмеження доступу до інформації для певних груп населення, що може порушити принципи рівноправності та справедливості;
- можливість зловживання владою та використання інформаційної політики задля підтримки конкретних політичних або економічних інтересів.

Наступним важливим документом, який визначає стратегічні напрями розвитку інформаційної безпеки в країні, є Указ Президента України № 47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України» [6]. Дана Доктрина відображає важливі аспекти, які визначають підходи та пріоритети в роботі над забезпеченням інформаційної безпеки України, а саме: загрози та виклики. В документі проаналізовано сучасні та можливі майбутні загрози для інформаційної безпеки України – інформаційну агресію, дезінформацію, кіберзагрози, військові дії в інформаційному просторі та ін. Пріоритети: документ описує ключові напрями і пріоритети дій в інформаційній безпеці. Міжнародне співробітництво, доктрина визнає важливість міжнародного співробітництва в галузі інформаційної безпеки. Вказується на необхідність співпраці з іншими державами та міжнародними організаціями у боротьбі з інформаційними загрозами. Також документ наголошує на важливості створення ефективного законодавчого та інституційного середовища для забезпечення інформаційної безпеки.

Водночас негативним аспектом даного документа є його загальність та відсутність конкретних стратегічних дій для впровадження зазначених пріоритетів. Наприклад, хоч і зазначається важливість кібербезпеки, не надається докладніша інформація щодо планів та програм в цьому напрямі. Важливим є питання забезпечення фінансування та координації заходів, що визначені в Доктрині.

Загалом, Доктрина інформаційної безпеки України відображає важливі аспекти розвитку інформаційної безпеки в країні, проте для її успішної реалізації необхідно враховувати конкретність та реалістичність стратегічних дій, а також забезпечити ефективну координацію та фінансування.

Актуальними проблемами інформаційної безпеки в Україні є різноманітні виклики та загрози, які виникають внаслідок широкого використання інформаційних технологій та впливають на різні сфери суспільства. До основних проблем варто віднести інформаційну агресію з боку Російської Федерації, адже Україна зіткнулася не лише з військовою, але й з інформаційною агресією та дезінформацією, спрямованою на дестабілізацію суспільства, зменшення довіри до державних інституцій та поширенням фейкової інформації. Кібератаки

та кіберзагрози, зростання кількості та складності кібератак на державні і корпоративні інфраструктури призводить до значних втрат інформації, порушення функціонування систем приватності громадян. Недостатній рівень цифрової грамотності населення спричиняє те, що громадяни стають вразливими до фішингу, кібершахрайства та інших онлайн-загроз. Відсутність належного захисту електронних систем державних органів може призвести до можливості кібернападів на державні структури, що в результаті порушить об'єктивне функціонування держави. Поширення фейкової інформації та дезінформації може викликати недовіру до джерел новин, загрожувати об'єктивності медіа та спотворювати образ країни. Недостатнє регулювання інтернет-простору, а саме відсутність ефективних механізмів контролю та регулювання інтернет-контенту, може призвести до поширення неправомірної інформації та порушення законів. Розв'язання цих проблем потребує комплексного підходу, включаючи розвиток кіберзахисту, підвищення цифрової грамотності, сприяння об'єктивності інформаційного простору, зміцнення законодавства та ефективну співпрацю між відомствами та суб'єктами господарювання.

Відповідно до Закону України «Про Національну програму інформатизації» [2] наявні небезпеки для національних інтересів та безпеки України в інформаційній сфері включають: спеціальні інформаційні операції, адже вчинення таких операцій спрямовано на ослаблення обороноздатності, деморалізацію військових формувань, провокування екстремізму, спричинення паніки, збільшення соціально-політичної та соціально-економічної нестабільності, стимулювання міжетнічних та міжрелігійних конфліктів в Україні. Держава-агресор впроваджує інформаційні операції в інших країнах для створення негативного враження про Україну у світі. Інформаційна експансія: країна-агресор зосереджується на розвитку власної інформаційної інфраструктури на території України та інших держав для здійснення інформаційного контролю. Держава-агресор здійснює інформаційний контроль на тимчасово окупованих територіях. Недостатній розвиток державної інформаційної інфраструктури – обмежена здатність реагувати на інформаційні атаки та активно діяти в інформаційному полі для захисту національних інтересів. Неефективна національна інформаційна політика – недостатність законів, що регулюють суспільні відносини в інформаційній сфері, відсутність стратегічного наративу та недостатній рівень культури соціальних медіа. Поширення заклику до радикальних дій: пропаганда концепцій ізоляціонізму та автономії в різних регіонах України [4].

Важливість системного підходу до забезпечення інформаційної безпеки та активної ролі держави у розробці та впровадженні стратегічних заходів у цій сфері є надзвичайно великою. Розвиток технологій та їх вплив на суспільство ставлять перед державою завдання забезпечити не лише фізичну безпеку, а й інформаційну, оскільки вразливість інформаційних систем може призвести до серйозних наслідків.

Системний підхід передбачає комплексне охоплення всіх аспектів інформаційної безпеки, від технічних аспектів захисту інформаційних систем до підвищення цифрової грамотності громадян та вдосконалення законодавства. Він охоплює взаємодію між різними суб'єктами (державні органи, приватний сектор, громадські організації) для координації зусиль у досягненні загальної мети – забезпеченні надійного та безпечного інформаційного середовища.

Активна роль держави є ключовою у цьому процесі. Держава повинна виступити ініціатором та координатором розвитку стратегічних заходів з інформаційної безпеки, сприяти розробці та впровадженню стандартів, регуляцій та законодавства, які б враховували сучасні технологічні виклики. Важливою складовою ролі держави є створення сприятливого інституційного середовища для розвитку інформаційної безпеки, залучення фахівців та інвестицій для вдосконалення інфраструктури та технологій.

Отже, системний підхід до забезпечення інформаційної безпеки та активна роль держави є необхідними для ефективного захисту інформаційного простору в умовах

висхідних технологічних загроз та викликів. Це сприятиме забезпеченню стійкого розвитку суспільства та захисту національних інтересів.

Вважаємо, що для розв'язання стратегічних проблем інформаційної безпеки України важливо розробити чітку та системну стратегію інформаційної безпеки, яка охоплює всі аспекти та сектори суспільства, включаючи державний сектор, громадянське суспільство та бізнес, створити центри аналізу та реагування на кіберзагрози, а саме впровадити національні центри, які будуть відстежувати, аналізувати та реагувати на кіберзагрози та атаки, забезпечуючи оперативне реагування на нові вектори атак, вдосконалити заходи з кібербезпеки для критично важливих об'єктів (енергетика, транспорт, фінанси, медичні системи тощо). Для запобігання можливим кібератакам забезпечити постійний моніторинг і аналіз нових тенденцій у сфері кібербезпеки для своєчасного виявлення та протидії потенційним загрозам, розробити й вдосконалити законодавчу базу в галузі кібербезпеки, що відповідає сучасним викликам та міжнародним стандартам.

Вважаємо, що ці напрями допоможуть створити більш ефективну систему захисту інформаційної безпеки в Україні та протидіяти потенційним загрозам.

Висновки. Проведений аналіз дає підстави зазначити, що сучасні проблеми інформаційної безпеки України відображають складний характер викликів, з якими зіткнулося цифрове суспільство країни. Зокрема, кіберзагрози, дезінформація, кібератаки та інші інформаційні виклики мають потенціал завдати шкоди як національній безпеці, так і громадській довірі. Для подолання цих викликів важливо використати системний підхід. Розвиток комплексної інформаційної стратегії, підвищення кіберграмотності населення, зміцнення кібербезпеки критично важливих об'єктів, міжнародна співпраця та створення відповідної правової бази – це лише деякі з напрямів, які допоможуть забезпечити національну інформаційну безпеку. Активна роль держави, спільні зусилля всіх галузей суспільства та уважний аналіз нових тенденцій є ключовими факторами у забезпеченні ефективного захисту від кіберзагроз та надійної інформаційної безпеки для розвитку країни.

Список використаних джерел:

1. Виздрик В., Мельник О. Інформаційна безпека в Україні. *Grail of Science*. 2023. № 24. С. 196–202. URL: https://doi.org/10.36074/grail-of-science.17.02.2023.034 (дата звернення: 22.08.2023).

2. Про Національну програму інформатизації: Закон України від 01.12.2022 р. №2807-IX. URL: https://zakon.rada.gov.ua/laws/show/2807-20#Text (дата звернення: 22.08.2023).

3. Залєвська І.І., Удренас Г.І. Інформаційна безпека в Україні в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1. С. 20–26.

4. Ніщименко О.А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. *Наше право*. 2016. № 1. С. 17–23.

5. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради Національної Безпеки і Оборони України від 18 березня 2022 р. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#Text (дата звернення: 22.08.2023).

6. Про Доктрину інформаційної безпеки України: Указ Президента України №47/2017 Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text (дата звернення: 22.08.2023).

REFERENCES

1. Vyzdryk, V., & Melnyk, O. (2023). Informatsiina bezpeka v Ukraini [Information security in Ukraine]. *Grail of Science*, *24*, 196–202. Retrieved from https://doi.org/10.36074/grail-of-science.17.02.2023.034 [in Ukrainian].

2. Pro Natsionalnu prohramu informatyzatsii: Zakon Ukrainy [On the National Informatization Program: Law of Ukraine] vid 01.12.2022 p. №2807-IX. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/2807-20#Text [in Ukrainian].

3. Zalievska, I.I., & Udrenas, H.I. (2022). Informatsiina bezpeka v Ukraini v umovakh rosiiskoi viiskovoi ahresii [Information security in Ukraine in the conditions of Russian military aggression]. *Pivdennoukrainskyi pravnychyi chasopys – South Ukrainian legal journal, 1,* 20-26 [in Ukrainian].

4. Nishchymenko, O.A. (2016). Informatsiina bezpeka Ukrainy na suchasnomu etapi rozvytku derzhavy i suspilstva [Information security of Ukraine at the current stage of development of the state and society]. *Nashe pravo – Our right, 1,* 17–23 [in Ukrainian].

5. Shchodo realizatsii yedynoi informatsiinoi polityky v umovakh voiennoho stanu: Rishennia Rady Natsionalnoi Bezpeky i Oborony Ukrainy vid 18 bereznya 2022 r. [Regarding the implementation of a unified information policy under martial law: Decision of the National Security and Defense Council of Ukraine from March 18, 2022]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/n0004525-22#Text [in Ukrainian].

6. Pro Doktrynu informatsiinoi bezpeky Ukrainy: Ukaz Prezydenta Ukrainy №47/2017 Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 r. [On the Information Security Doctrine of Ukraine: Decree of the President of Ukraine On the decision of the National Security and Defense Council of Ukraine from December 29, 2016]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/47/2017#Text [in Ukrainian].

Подано до редакції 6.04.2023 р.
Прийнято до друку 17.05.2023 р.