Гуманітарна і політична безпека держави

УДК 342.7

**Хромова Юлія Олександрівна**
*кандидат наук з державного управління,*
*доцент кафедри публічного управління та регіоналістики*
*Національний університет «Одеська політехніка»*
**Khromova Yuliia**
*PhD in Public Administration, Associate Professor of the*
*Department of Public Administration and Regional Studies*
*Odesa Polytechnic National University*
*ORCID: 0000-0003-3761-2169*

# ПРІОРИТЕТНІ ЗАВДАННЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ РИЗИКІВ ТА ЗАГРОЗ: СУЧАСНИЙ ВИМІР
# PRIORITY TASKS OF ENSURING INFORMATION SECURITY IN THE CONDITIONS OF RISKS AND THREATS: THE MODERN DIMENSION

***Анотація.*** *Глобальна нестабільність та швидкі трансформації у суспільстві потребують своєчасного оновлення відповідних інструментів, методів, засобів та векторів протидії різноманітним атакам, які здійснюють деструктивний вплив на інформаційні ресурси та інфраструктуру приватного та публічного секторів. Визначено, що одним із ключових національних інтересів виступає розвиток національного інформаційного простору, який діє в умовах забезпечення належного захисту від загроз та ризиків.*

*Мета. Метою дослідження є аналіз сценаріїв розповсюдження дезінформації та маніпулювання інформацією в українському інформаційному просторі з боку країни-агресора, встановлення завдань*

*забезпечення інформаційної безпеки в сучасних умовах загроз та ризиків, розробка пропозиції щодо удосконалення забезпечення інформаційної безпеки в Україні.*

*Матеріали і методи. Серед матеріалів дослідження було використано такі, як: 1) нормативно-правові акти з питань забезпечення інформаційної безпеки; 2) науково-практичні праці вітчизняних та зарубіжних авторів, які досліджують питання захисту інформаційного простору та забезпечення інформаційної безпеки. В ході дослідження використовувались такі методи: аналіз і синтез – при визначенні загроз та ризиків забезпечення інформаційної безпеки, простеженні взаємозв'язків дезінформації та активних дій для реалізації країною-агресором власних цілей на території України; системно-аналітичний – для аналізу нормативно-правових актів, які регламентують питання забезпечення інформаційної безпеки в країні.*

*Результати. Досліджено загрози та ризики інформаційної безпеки країни, що існують в сучасних умовах повномасштабного вторгнення країни-агресора до України. Закцентовано увагу на хакерських атаках на публічні веб-портали та сервери, а також на розповсюдження дезінформації через засоби масової інформації та соціальні мережі з боку рф. З'ясовано, що діяльність країни-агресора у ЗМІ та в різних соціальних мережах проводилась проти України щодо дестабілізації ситуації у суспільстві та з метою його розколу ще з насів набуття нею незалежності. Проаналізовано їх вплив на українське населення на східних та південних територіях. Підкреслено, що ключовою основою зовнішньої пропагандистської політики країни-агресора стосовно України полягала у використанні етнокультурного фактору.*

*Перспективи. У проведенні подальших наукових досліджень слід зосередитись на видах правової відповідальності, яка має бути застосована до порушників інформаційної безпеки держави, суспільства,*

*людини, та має виступати гарантією забезпечення національної стабільності, дотримання цифрових прав громадян.*

***Ключові слова**: інформаційна безпека, загрози, ризики, деструктивна інформація, пропаганда.*

***Summary.** Global instability and rapid transformations in society require a timely update of appropriate tools, methods, means and vectors for countering various attacks that have a destructive effect on information resources and infrastructure of the private and public sectors. It was determined that one of the key national interests is the development of the national information space, which operates under the conditions of ensuring adequate protection against threats and risks.*

*Purpose. The purpose of the study is to analyze the scenarios of the spread of disinformation and manipulation of information in the Ukrainian information space by the aggressor country, to establish the tasks of ensuring information security in modern conditions of threats and risks, to develop a proposal for improving the provision of information security in Ukraine.*

*Materials and methods. Among the research materials, the following were used: 1) normative legal acts on information security issues; 2) scientific and practical works of domestic and foreign authors, which investigate the issues of protection of information space and provision of information security. During the research, the following methods were used: analysis and synthesis - when determining threats and risks of ensuring information security, tracing the interrelationships of disinformation and active actions for the aggressor country to realize its own goals on the territory of Ukraine; system-analytical - for the analysis of normative legal acts that regulate the issue of ensuring information security in the country.*

*Results. Threats and risks of the country's information security that exist in modern conditions of a full-scale invasion of the aggressor country into Ukraine*

*have been studied. Attention is focused on hacker attacks on public web portals and servers, as well as on the spread of disinformation through mass media and social networks by the Russian Federation. It was found that the activities of the aggressor country in the mass media and in various social networks were carried out against Ukraine in order to destabilize the situation in society and with the aim of splitting it even before it gained independence. Their impact on the Ukrainian population in the eastern and southern territories is analyzed. It is emphasized that the key basis of the foreign propaganda policy of the aggressor country in relation to Ukraine was the use of the ethno-cultural factor.*

*Discussion. In conducting further scientific research, one should focus on the types of legal responsibility that should be applied to violators of the information security of the state, society, and person, and should act as a guarantee of ensuring national stability and the observance of the digital rights of citizens.*

***Key words:*** *information security, threats, risks, destructive information, propaganda.*

**Постановка проблеми.** Інформація є найціннішими ресурсом у світі впливів, яка характеризується мультифункціональним поширенням сфер для її застосування, зокрема у соціально-економічній, освітній, культурній, публічно-управлінській сфері, а також інших суспільно важливих напрямах. Враховуючи глобальну нестабільність та швидкі трансформаційні зміни суспільства, оновлюються також інструменти, методи, засоби, вектори протидії різноманітних атак, що деструктивно впливають на інформаційні ресурси та відповідну інфраструктуру як публічного сектору, так і приватного. Зрозуміло, що застосування нових інформаційних технологій тягне за собою відповідну зміну традиційних парадигм, визначаючи нові правила у використанні інформаційних систем.

Ґрунтуючись на Стратегії національної безпеки України [2] слід визначити інформаційну безпеку складовою національної безпеки, що підкреслює її пріоритетний напрямок впровадження провідних інформаційних технологій, які покращують добробут громадян та економіку країни загалом. Так, розвиток національного інформаційного простору є одним з ключових національних інтересів, в умовах забезпечення належного захисту від загроз та ризиків. Проривні цифрові технології XXI століття активно корелюються з безмежними можливостями розвитку держави та суспільства, при цьому створюючи також нові форми викликів та загроз забезпечення безпеки функціонування цих технологій.

Кількість порушень, пов'язаних з інформаційними технологіями, кожного року лише зростає, так, у 2022 році було виявлено 7,9 тис. правопорушень, а за 2023 рік це число зросло до 45,7 тис. [8], значна частина яких складає виявлення кібершахрайств [5, с. 83-87].

Зазначене, підкреслює потенційну можливість застосування сучасних інформаційних технологій з метою дотримання принципів: а) відмови від невтручання у внутрішні справи іншої держави; б) від застосування заходів сили; в) забезпечення прав і свобод громадянина.

**Аналіз останніх досліджень і публікацій**. При дослідженні загроз та ризиків інформаційному простору та забезпечення інформаційної безпеки важливе значення мали напрацювання фахівців, які займались визначенням сучасних загроз інформаційної безпеки, проблем захищеності інформаційних систем, особливості інформаційної безпеки в умовах військової агресії тощо: О. Бєлов [9], О. Бодунова [5], Е. Вілсон [6], В. Гобела [12], В. Гребенюк [9], А. Клочко [10], В. Котляров [11], Г. Леськів [12], С. Лихова [15], В. Новородовський [13], О. Свідерська [14], В. Сисоєва [15], Я. Усов [17], Л. Філіпішина [18], І. Шопіна [19], A. Kramer [20] та ін.

В. Новородовський [13, с. 150-179] у своєму дослідженні акцентує увагу, що використання певних проблемних питань, які існують у

відповідній країні, надає можливість стороннім суб'єктам формувати серед населення незадоволеність, що сприяє формуванню маніпулятивних передумов для задоволення власних (ворожих) амбіції у політичній площині.

Я. Усов [17, с. 145-151], досліджуючи проблеми захищеності інформаційного середовища, зазначає, що реальність певної загрози для інформаційної безпеки перманентно проявляється у ризику, який пов'язаний з використанням певних вразливих секторів інформаційних активів, що спричинює державі, суспільству, людині відповідні збитки.

М. Дзевелюк, Є. Костик та Л. Філіпішина [18, с. 196-205] підкреслюють, що військова агресія рф спонукала на встановлення нових вимог захисту інформаційної безпеки. Тому для ефективної діяльності у цій сфері автори пропонують запровадити: а) загальні стандарти, забезпечені нормативно-правовим підґрунтям; б) систему проведення моніторингу можливих загроз.

В. Котляров [11, с. 131-124] вказує, що в умовах сьогодення чинником суспільного життя виступає саме інформаційна сфера, що впливає на економічний, політичний, воєнний сектор держави. Автор встановлює, що в інформаційному просторі всі користувачі інформаційних технологій обов'язково мають дотримуватись відповідних вимог забезпечення внутрішньої та зовнішньої безпеки.

В. Сисоєва та С. Лихова [15, с. 102-107], досліджуючи діяльність правоохоронних органів у сфері забезпечення інформаційної безпеки, зазначають, що застосування методів адміністративного регулювання у зазначеній сфері вказують на наявність певної управлінської системи, що здійснює вплив на захист інформаційного простору через попередження та/або оперативне відвернення можливих загроз. Автори також вказують на актуальність вирішення питання щодо розробки відповідних механізмів та інструментів для удосконалення та оптимізації правового підґрунтя для реалізації державної політики забезпечення інформаційної безпеки.

На думка А. Клочка [10, с. 38-42], стратегічним завданням держави виступає необхідність впровадження певного механізму, який має забезпечити інформаційну безпеку через реалізацію відповідної системної діяльності, сукупності певних заходів, функціонування інституцій державного-правового спрямовування, завдяки чому гарантуватимуть захист національних інтересів, інтересів суспільства і людини, вживати заходів попередження інформаційних загроз та їх швидкого подолання.

І. Шопіна [19, с. 28-35] вказує, що інформаційна безпека передбачає собою таку ідеальну модель середовища, в якому немає місця будь-яким інформаційним загрозам. За таких умов впроваджуються сучасні цифрові технології майже у всі сфери суспільного життя з метою забезпечення реалізації інформаційних прав та інтересів як фізичних, так і юридичних осіб. Таким чином, автор розкриває забезпечення інформаційної безпеки як певної сукупності дій відповідних державних органів, громадського суспільства, громадян, які націлені на проведення діяльності щодо інформаційної обізнаності суб'єктів-користувачів інформаційних технологій.

При цьому Г. Леськів, В. Гобела, Н. Лесик [12], звертають увагу на ключову роль у подоланні загроз інформаційної безпеки як сучасних технічних засобів та відповідного оснащення, так й високий рівень інформаційної обізнаності персоналу та громадян, що обумовлено динамічним зростанням інформаційних технологій та виникненням нових видів загроз.

Попри наявності значної кількості праць із зазначеного питання, є потреба дослідити пріоритетні завдання забезпечення інформаційної безпеки в умовах сучасних ризиків та загроз, розробити практичні рекомендації щодо подальшої протидії їм.

**Метою дослідження** є: аналіз сценаріїв розповсюдження дезінформації та маніпулювання інформацією в українському інформаційному просторі з боку країни-агресора, встановлення завдань

забезпечення інформаційної безпеки в сучасних умовах загроз та ризиків, розробка пропозиції щодо удосконалення забезпечення інформаційної безпеки в Україні.

Відповідно до мети були визначені такі завдання:

– проаналізувати сценарії розповсюдження дезінформації та маніпулювання інформацією в українському інформаційному просторі з боку країни-агресора;

– встановити особливості спрямування загроз інформаційній сфері України, які реалізуються країною-агресором;

– розробити пропозиції щодо удосконалення забезпечення інформаційної безпеки в Україні.

**Матеріали і методи.** Серед матеріалів дослідження було використано такі, як: 1) нормативно-правові акти з питань забезпечення інформаційної безпеки; 2) науково-практичні праці вітчизняних та зарубіжних авторів, які досліджують питання захисту інформаційного простору та забезпечення інформаційної безпеки. В ході дослідження використовувались такі методи: аналіз і синтез – при визначенні загроз та ризиків забезпечення інформаційної безпеки, простеженні взаємозв'язків дезінформації та активних дій для реалізації країною-агресором власних цілей на території України; системно-аналітичний – для аналізу нормативно-правових актів, які регламентують питання забезпечення інформаційної безпеки в країні.

**Виклад основного матеріалу.** Сучасне забезпечення інформаційної безпеки характеризується як комплексна система, яка обумовлена впливом багаточисленних факторів та кібернетичних загроз. Звернемо увагу, що стрімкий розвиток інформаційно-телекомунікаційних технологій, передусім, передбачав лише позитивний вплив на життєдіяльність суспільства та затвердився як ефективний інструмент творення, проте включає в себе певні ризики. Відтак, особливості забезпечення інформаційної безпеки полягають у формуванні надійного нормативно-

правового фундаменту та запровадження відповідних заходів щодо захисту інформаційного простору, при цьому, визначимо проблему узгодженості міжнародних норм з національним правовим простором в інформаційній сфері. Це розкриває завдання держави, а саме її правової системи, щодо реального осмислення інформаційних новел та цифрових технологій, та формування відповідних правил регулювання суспільних відносин у цій сфері, з метою забезпечення розвитку країни.

Слід враховувати, що умови сьогодення, обумовлені повномасштабним вторгненням військ рф на територію України 24 лютого 2022 року, які суттєво вплинули як на кількість, так і на зміст порушень безпеки в інформаційній сфері. Так, серед факторів, що впливають на вразливість інформаційної безпеки, можна виокремити такі, як: хакерські атаки на публічні веб-портали та сервери; викрадення відповідних даних; цифрове шпигунство; зараження вірусами програмних засобів та систем тощо. За даними департаменту кібербезпеки Служби безпеки України зафіксовано близько 10 тис. кібернетичних атак [16], починаючи з початку 2022 року, на інформаційні об'єкти в Україні з боку країни-агресора. Отже, доцільно визначати такі дії як кібернетичну війну, що представляє собою певний конфлікт, який існує в інформаційно-телекомунікаційному просторі, використовуючи при цьому відповідні комп'ютерні технології з метою дестабілізації інформаційної інфраструктури, збирання даних, пошкодження або знищення важливих мереж та систем. Такі дії супротивника можуть завдати значної шкоди як національній безпеці країни, так й її економічній сфері. Відтак, слід вважати, що активне проведення різних DOS-атак або хакерських атак, інших спланованих операцій на українські інформаційні ресурси свідчить про зневагу до інформаційного суверенітету нашої країни.

Таким чином, забезпечення інформаційної безпеки має на меті формування відповідних правових умов для послідовної реалізації інтересів

індивідів, суспільства, держави в межах державної політики розвитку інформаційного суспільства в умовах забезпечення заборони стороннього деструктивного втручання.

Однак, слід підкреслити, що широке поширення отримало розповсюдження дезінформації, інформаційної маніпуляції (ще з 2014 року) в соціальних мережах «Телеграм», «Фейсбук», що значно підвищує їх ефективність, оперативність, деструктивний вплив майже на всі сфери життя суспільства та функціонування держави. У даному випадку, слушною є думка Е. Вілсона щодо визначення сучасних медіа-технологій як платформи «для пропаганди та брехні, які тягнуть за собою війни» [6]. Враховуючи кількість користувачів у різних соціальних мережах, легко оцінити ефективність використання різноманітних маніпулятивних заходів. Відтак, зазначене ґрунтується, по-перше, на завчасній інформаційній діяльності в українському суспільстві щодо формування у населення відкидаючого мислення по відношенню до України, та лояльного сприйняття політики країни-агресора, по-друге, призвело до дестабілізації внутрішньої ситуації у нашій державі, формування груп проросійського спрямування.

Зазначимо, що аналогічний сценарій інформаційних маніпуляцій був апробований у конфліктах у Придністров'ї, Нагорному Карабасі, Грузіїї, проте в Україні це отримало найбільший рівень ефективності через суттєвий розвиток к 2022 року інформаційних (цифрових) технологій, інформаційно-телекомунікаційних систем та значно більшої кількісті користувачів соціальних мереж. Адже, країною-агресором, поки це було можливо, активно використовувалися поширені на пострадянському просторі соціальні мережі «одноклассники» та «вконтакте», через які постійно розповсюджувались дезорганізуючі наративи щодо «унікального провідного» положення нації країни-агресора. Отже, були створені

необхідні та потужні умови для ведення гібридної війни, сепаратистських рухів в інших країнах, зокрема в Україні.

Діяльність країни-агресора у ЗМІ, а з часом і в різних соціальних мережах, проти України щодо дестабілізації ситуації у суспільстві та з метою його розколу, почалась ще з часів отримання незалежності нашою країною. Підкреслимо, що країна-агресор висвітлювала громадян України нацистами, поширювали (недостовірну) інформацію про переслідування російськомовних громадян, наводила історичні та/або інформаційні факти, які не відповідали реальності, проте формували в суспільстві дискримінаційні думки, які підсилювались «замовними коментарями» з боку «ботів» та «тролів» [14, с. 60-65]. Зрозуміло, що рф активно використовувала етнокультурний фактор у реалізації своєї зовнішньої пропагандистської політики, спираючись на ту частку російськомовного населення та росіян, що мешкали в Україні. «Маніпулюючи історичною пам'яттю та спекулюючи, мовним питанням російська пропаганда створила умови для конфлікту на етнічному ґрунті».

Однак, все це було б неможливим без сприяння деяких українських політиків та посадовців, які час від часу підтверджували необхідність російського втручання у справи нашої країни. Це, передусім, підтверджується подіями 2014 року. Революція Гідності стала відправною точкою застосування рф відкритою агресію, маючи за мету організувати громадянську війну, з метою руйнування й поглинання України [9, с. 57].

22 лютого 2014 року депутати південно-східних областей України від «Партії регіонів» (Харківська, Луганська, Донецька області, Автономна Республіка Крим та ін.) мали за мету «взяти усе в свої руки», створивши відповідні народні республіки. Висновки цієї зустрічі нам відомі: не маючи необхідної підтримки з боку суспільства, керівники Харківської області відмовились від участі у порушені конституційного устрою країни. Проте,

депутати партії в АРК почали активно реалізовувати досягнуті на з'їзді домовленості.

Так, 26 лютого вже проходили в Сімферополі та Севастополі малочислені мітинги (для створення інформаційного приводу), які ґрунтувались на попередніх домовленостях з країною-агресором та її запрошенням «навести порядок». Користуючись наявністю на території автономії своїх військових частин та морської військової бази, вони завчасно перемістили до них значну частину військової техніки, зокрема, танків, та зброї. Тому, територія півострова легко була окупована російськими військами, а на референдумі 18 березня 2014 року вже вирішено питання про вступ Криму до складу рф. Адже Крим завжди, а після 1991 року зокрема, тягнув до себе офіцерів у відставці та мешканців північних регіонів рф, які виступили головною силою, що підтримали сепаратистів. Важливо зазначити, що проведенню активних наступальних дій передувало ретельна підготовка російськомовного населення через ЗМІ та соціальні мережі до «ідеї об'єднання, поновлення їх території, проживання в складі рф».

Таким чином, завдяки завчасній підготовці населення до подій щодо об'єднання територій через засоби масової інформації та соціальні мережі, а також поширенню за радянською калькою картинки «відчуття щастя» від цього, цепною реакцією проявило підтримку сепаратистів населенням півострова.

Швидко отримавши потрібний країні-агресору результат з Кримом, було вирішено «повторити» теж саме в Луганській та Донецькій областях і 13 квітня 2014 року почався наступ, проте, населення не було готово до такого повороту подій, їх там не чекали, та й українська держава вже не мала наміру віддавати ці території. Тоді щасливі картинки об'єднання Криму з рф стали змінюватись іншими, викривленими фактами, наприклад, використанням фотознімків конфліктів на інших територіях, їх жертв, з

подачею такого змістовного значення, щоб звинуватити у цьому українську сторону та спровокувати суспільне обурення з певного приводу. Однак, навіть через спростування подібної інформації українськими експертами, така дезінформація мала негативний вплив як на суспільство, так і на міжнародний імідж країни.

Зараз зрозуміло, що певне «замороження» конфлікту на сході призвело до корегування планів країни-агресора щодо захоплення України, накопичення військових ресурсів, поширення власної ідеології на російськомовне населення через соціальні мережі та завдяки сучасним інформаційним технологіями. Відтак, потреба у захисті українського інформаційного простору спонукала до розробки відповідного нормативного підґрунтя. Так, важливого значення набув Указ Президента України «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» № 133/2017 [1], через запровадження заборон на сайти та соціальні мережі російських власників. До списку блокування увійшли «яндекс», «одноклассники», «вконтакте», «mail.ru», «антивірус Касперського», антивірус «Dr. Web», система обліку «1С».

Наведені зміни значно вплинули на поглинання українцями російської пропаганди через соціальні мережі та інформаційні ресурси, однак, зазначені заборони не зупинили країну-агресора в просуванні своєї пропаганди через інформаційні мережі, і з часом вони розвернули активну діяльність спочатку у групах месенджеру Viber, а з часом, зокрема, під час повномасштабного вторгнення рф на територію України, інформаційні потоки надходили з месенджеру Telegram. Отже, слід вважати, що домінуюча роль відведена в російсько-українському конфлікті саме інформаційним ресурсам, оскільки науковці довели можливість здійснювати керування людськими емоціями завдяки інформації у

соціальних мережах [20, с.8788-8790], що дозволяє легко маніпулювати свідомістю людей. Зрозуміло, що зазначена форма впливу представляє внутрішню загрозу для нашої країни та інструмент для дискредитації особи чи конкретного об'єкта атаки. Тому, в умовах сьогодення проводиться активне обговорення депутатами Верховної Ради України питань щодо обмеження функціонування цієї соціальної мережі на нашій території, як засобу забезпечення інформаційної безпеки.

Варто зазначити, що розповсюдження пропаганди з боку країни-агресора відбувається по всьому світу, через фальсифікацію даних та/або викривлення події та обставин, що формує у населення інших країн невідповідну дійсності оцінку ситуації. Разом з тим, слід враховувати, що розгортання відповідної інформації поширюється соціальними мережами, веб-порталами та іншими інформаційно-телекомунікаційними системами, які зареєстровані та знаходяться в іншій країні світу, через що суттєво впливає на уразливість українського інформаційного простору до загроз.

Виходячи з цього, визначимо такі типи інформації, які несуть негативний вплив для інформаційної безпеки, так це: а) інформація, завдяки якій здійснюються заклики до війни; б) інформація, що містить пропагандистські наративи ненависті до іншої соціальної групи; в) інформація, що містить провокацію до розпалення расової, етнічної, соціальної, релігійної, національної або іншої ворожнечі.

В умовах сьогодення захист суспільства від інформаційної небезпеки вирішується положеннями Доктрини інформаційної безпеки та Стратегії кібербезпеки України, якими закладено ключовий вектор забезпечення функціонування як кібернетичного простору України, так і протиборства інформаційній агресії з боку рф. Доцільно враховувати, що забезпечення інформаційної безпеки держави, суспільства та громадян є основою для захисту їх прав на володіння та розпорядження інформацією. Відтак, застосування концептуального підходу до нормативно-правового

регулювання забезпечення інформаційної безпеки сприятиме збалансуванню та зміцненню державної системи захисту інформаційного простору.

Проаналізувавши зазначені нормативні документи, виокремимо головні вектори діяльності щодо інформаційної безпеки: 1) формування захищеного кібернетичного простору; 2) забезпечення захисту об'єктів критичної інфраструктури, державної інформаційної інфраструктури та електронних ресурсів; 3) протидія поширенню кіберзлочинності [3]; 4) захист українського інформаційного простору від агресивного впливу деструктивної пропаганди, а також «пропаганди війни, національної чи релігійної ворожнечі…» з боку країни-агресора [4].

Разом з тим, зафіксовані вектори забезпечення інформаційної безпеки представляють собою узагальненні формулювання, які не розкривають конкретні заходи здійснення такої діяльності, зокрема контроль та прогнозування захищеності інформаційних ресурсів держави, вирішення питань щодо виявлення, попередження, усунення наслідків кібернетичних атак на інформаційні ресурси в Україні та інше. Так, з метою протистояння активній пропаганді країни-агресора, вкрай необхідним є напрацювання потужного нормативного підґрунтя для захисту українського інформаційного простору в умовах сьогодення.

Відтак, відомі інструменти вчинення інформаційного впливу на людей, які використовує країна-агресор, мають бути заблоковані та заборонені в України, відповідно мають бути прийняті дієві правові норми, для їх виявлення, заборони та змушення власників інформаційних платформ застосувати більш жорсткі модернізаційні протоколи щодо дезінформаційного контенту. При цьому вважаємо, що захист інформаційного простору доцільно здійснювати через блокування відповідних платформ, що мають загальний доступ до інформації, але в умовах сьогодення не врегульовані законодавством, тому їх провайдери (що

не є суб'єктами медіа галузі) не несуть відповідальності за порушення захисту персональних даних українців, не здійснюють блокування незаконного контенту чи поширення інформації, яка не є достовірною. Тому, слід підтримати розгляд законопроекту від 25.03.2024 року № 11115 «Про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація» [7]. Завдяки зазначеним новелам стане можливим блокуванням таких інформаційних ресурсів, як анонімні телеграм-канали російських пропагандистів, телеграм-канали російських медіа.

Варто підкреслити, що наразі Державна служба спеціального зв'язку та захисту інформації України планує запровадити систему блокування російського теле-і радіо сповіщення на прикордонних територіях східної України.

Відтак, вважаємо, що законодавче поле має бути підсиленим у цьому питанні, забезпечуючи захист даних, що зберігаються в інформаційно-телекомунікаційних системах. Таким чином, доцільним вбачається запровадження незалежних та самостійних засобів для проведення моніторингу забезпечення інформаційної безпеки України з метою своєчасного та ефективного контролю за станом захищеності інформаційних систем та інфраструктури, що спрямовано на нейтралізацію інформаційних ризиків та загроз через їх оперативне усунення.

**Висновки і перспективи подальших досліджень.** Підсумовуючи наведене, зазначимо, що досліджені питання забезпечення інформаційної безпеки в умовах сучасних загроз вимагають запровадження нових інструментів протидії ризикам та загрозам, що надходять з боку країни-агресора. Встановлено, що розвиток безпечного інформаційного простору, захист населення від деструктивного інформаційного впливу, захист інформаційних ресурсів та недопущення інформаційних загроз та ризиків,

виступають ключовим завданням української держави в умовах інформаційної війни.

Рекомендовано, посилити дієвість правових норм для притягнення до відповідальності осіб (зокрема юридичних осіб) – власників інформаційних платформ за порушення спільного доступу до інформації, через які поширюється масова інформація. Запровадити для них адміністративні штрафи та вимоги щодо підзвітності державним службам в інформаційній сфері. Доповнити Закону України «Про медіа» нормою щодо обмеження розповсюдження програм або інформації користувачів на своїй платформі спільного доступу за вимогою відповідного державного органу – Національної ради з питань телебачення та радіомовлення. Проводити постійний моніторинг оголошень, інформації, фото-, відео-матеріалів у поширених на території України месенджерах (наприклад, Viber), застосунках (наприклад, OLX) на предмет розміщення об'єкта, що містить дезінформацію, символіку країни-агресора, інші інформаційні та провокаційні матеріали, що вказують на підтримку рф.

## Література

1. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Указ Президента України від 15.05.2017 р. № 133/2017. URL: http://zakon.rada.gov.ua/laws/show/133/2017#Text (дата звернення: 26.06.2024).
2. Про рішення Ради національної безпеки і оборони України від 14 вересня 2020 року "Про Стратегію національної безпеки України": Указ Президента України від 14.09.2020 р. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text (дата звернення: 26.06.2024).

3. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 р. № 447/2021. URL: http://www.president.gov.ua/documents/4472021-40013 (дата звернення: 26.06.2024).

4. Стратегія інформаційної безпеки: Указ Президента України від 28.12.2021 р. URL: https://www.president.gov.ua/documents/3922020-35037 (дата звернення: 26.06.2024).

5. Бодунова О. Запобігання злочинності у сфері інформаційних технологій в умовах воєнного стану в Україні. *Науковий вісник Ужгородського університету: серія: Право.* 2023. Т.2. Вип. 75. С. 83-87. https://dspace.uzhnu.edu.ua/jspui/handle/lib/52678 (дата звернення: 26.06.2024).

6. Вілсон Е. Сім смертних гріхів, або Сім причин, чому Європа неправильно розуміє російсько-українську кризу. URL: https://cutt.ly/saXrq16 (дата звернення: 26.06.2024).

7. Законопроект від 25.03.2024 року № 11115 «Про внесення змін до деяких законів України щодо регулювання діяльності платформ спільного доступу до інформації, через які поширюється масова інформація». *Верховна Рада України: вебпортал.* URL: http://itd.rada.gov.ua/billInfo/Bills/Card/43884 (дата звернення: 26.06.2024).

8. Звіт національної поліції України про результати роботи у 2023 році. *Кабінет Міністрів України: вебсайт.* URL: www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf (дата звернення: 26.06.2024).

9. Ідеологічне та квазіправове обґрунтування Російською Федерацією анексії Автономної Республіки Крим / упоряд. : О. Бєлов, С. Кудінов, В. Гребенюк та ін. Київ : Нац. акад. СБУ, 2017. 284 с.

10. Клочко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної академії управління персоналом. Політичні науки та публічне управління.* 2022. 3 (63). С. 38-42.

11. Котляров В. Теоретичні засади сутності та концепції інформаційної безпеки. *Наукові перспективи.* 2023. № 6 (36). С. 131-142. doi: https://doi.org/10.52058/2708-7530-2023-6(36)-131-142.

12. Леськів Г., Гобела В., Лесик Н. Характеристика основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. *Економіка і право.* 2022. № 3. doi: https://doi.org/10.32782/2524-0072/2022-43-8.

13. Новородовський В. Інформаційна безпека України в умовах російської агресії. *Society. Document. Communication*. A series of «Historical science». 2020. Ed. 9. P. 150-179. doi: https://doi.org/10.31470/2518-7600-2020-9-150-179.

14. Свідерська О. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. *Науковий журнал "Політикус".* 2022. № 2. С. 60-65. doi: https://doi.org/10.24195/2414-9616.2022-2.10.

15. Сисоєва В., Лихова С. Діяльність правоохоронних органів України у сфері забезпечення інформаційної безпеки. *Scientific works of National Aviation University. Series: Law Journal "Air and Space Law".* 2022. № 3 (64). С. 102-107. doi: 10.18372/2307-9061.64.16896.

16. Служба безпеки цьогоріч нейтралізувала вже понад 3,5 тисячі кібератак. *Укрінформ.* URL: http://www.ukrinform.ua/rubric-technology/3594921-sluzba-bezpeki-cogoric-nejtralizuvala-vze-ponad-35-tisaci-kiberatak.html.

17. Усов Я. Проблеми захищеності інформаційного середовища. *Technical sciences and technologies.* 2019. № 1 (15). С.145-151. doi: 10.25140/2411-5363-2019-1(15)-145-151.

18. Філіпішина Л., Костик Є., Дзвелюк М. Публічне управління у сфері інформаційної безпеки (подолання сучасних загроз). *Актуальні питання у сучасній науці.* 2023. № 5. С. 196-205. doi: https://doi.org/10.52058/2786-6300-2023-5(11)-196-205.

19. Шопіна І. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ.* 2023. Вип. 1. С. 28-35. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/5636 (дата звернення: 26.06.2024).

20. Kramer A. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America*. 2014. 111 (24). P. 8788-8790. doi: 10.1073/pnas.1320040111.

## References

1. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 28 kvitnia 2017 roku «Pro zastosuvannia personalnykh spetsialnykh ekonomichnykh ta inshykh obmezhuvalnykh zakhodiv (sanktsii): Ukaz Prezydenta Ukrainy vid 15.05.2017 r. № 133/2017. URL: http://zakon.rada.gov.ua/laws/show/133/2017#Text [in Ukrainian].

2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 veresnia 2020 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy": Ukaz Prezydenta Ukrainy vid 14.09.2020 r. № 392/2020. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text [in Ukrainian].

3. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku «Pro Stratehiiu kiberbezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 26.08.2021 r. № 447/2021. URL: http://www.president.gov.ua/documents/4472021-40013 [in Ukrainian].

4. Stratehiia informatsiinoi bezpeky: Ukaz Prezydenta Ukrainy vid 28.12.2021 r. URL: https://www.president.gov.ua/documents/3922020-35037 [in Ukrainian].

5. Bodunova O. Zapobihannia zlochynnosti u sferi informatsiinykh tekhnolohii v umovakh voiennoho stanu v Ukraini. *Naukovyi visnyk Uzhhorodskoho universytetu: seriia: Pravo.* 2023. T.2. Vyp. 75. S. 83-87. https://dspace.uzhnu.edu.ua/jspui/handle/lib/52678 [in Ukrainian].

6. Vilson E. Sim smertnykh hrikhiv, abo Sim prychyn, chomu Yevropa nepravylno rozumiie rosiisko-ukrainsku kryzu. URL: https://cutt.ly/saXrq16 [in Ukrainian].

7. Zakonoproekt vid 25.03.2024 roku № 11115 «Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo rehuliuvannia diialnosti platform spilnoho dostupu do informatsii, cherez yaki poshyriuietsia masova informatsiia». *Verkhovna Rada Ukrainy: vebportal.* URL: http://itd.rada.gov.ua/billInfo/Bills/Card/43884 [in Ukrainian].

8. Zvit natsionalnoi politsii Ukrainy pro rezultaty roboty u 2023 rotsi. *Kabinet Ministriv Ukrainy: vebsait.* URL: www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2023/zvit_NPU_2023.pdf [in Ukrainian].

9. Ideolohichne ta kvazipravove obgruntuvannia Rosiiskoiu Federatsiieiu aneksii Avtonomnoi Respubliky Krym / uporiad.: O. Bielov, S. Kudinov, V. Hrebeniuk ta in. Kyiv: Nats. akad. SBU, 2017. 284 s. [in Ukrainian].

10. Klochko A. Zabezpechennia informatsiinoi bezpeky v umovakh suchasnoho suspilstva. Naukovi pratsi Mizhrehionalnoi akademii upravlinnia personalom. *Politychni nauky ta publichne upravlinnia.* 2022. 3 (63). S. 38-42 [in Ukrainian].

11. Kotliarov V. Teoretychni zasady sutnosti ta kontseptsii informatsiinoi bezpeky. *Naukovi perspektyvy.* 2023. № 6 (36). S. 131-142. doi: https://doi.org/10.52058/2708-7530-2023-6(36)-131-142 [in Ukrainian].

12. Leskiv H., Hobela V., Lesyk N. Kharakterystyka osnovnykh problem zabezpechennia informatsiinoi bezpeky v umovakh vplyvu tsyfrovykh tekhnolohii. *Ekonomika i pravo.* 2022. № 3. doi: https://doi.org/10.32782/2524-0072/2022-43-8 [in Ukrainian].

13. Novorodovskyi V. Informatsiina bezpeka Ukrainy v umovakh rosiiskoi ahresii. *Society. Document. Communication. A series of «Historical science».* 2020. Ed. 9. P. 150-179. doi: https://doi.org/10.31470/2518-7600-2020-9-150-179 [in Ukrainian].

14. Sviderska O. Tsyfrova propahanda ta ryzyky informatsiinoi bezpeky u konteksti rosiisko-ukrainskoi viiny. *Naukovyi zhurnal "Politykus".* 2022. № 2. S. 60-65. doi: https://doi.org/10.24195/2414- 9616.2022-2.10 [in Ukrainian].

15. Sysoieva V., Lykhova S. Diialnist pravookhoronnykh orhaniv Ukrainy u sferi zabezpechennia informatsiinoi bezpeky. *Scientific works of National Aviation University. Series: Law Journal "Air and Space Law".* 2022. № 3 (64). S. 102-107. doi: 10.18372/2307-9061.64.16896 [in Ukrainian].

16. Sluzhba bezpeky tsohorich neitralizuvala vzhe ponad 3,5 tysiachi kiberatak. *Ukrinform.* URL: http://www.ukrinform.ua/rubric-technology/3594921-sluzba-bezpeki-cogoric-nejtralizuvala-vze-ponad-35-tisaci-kiberatak.html [in Ukrainian].

17. Usov Ya. Problemy zakhyshchenosti informatsiinoho seredovyshcha. *Technical sciences and technologies.* 2019. № 1 (15). S.145-151. doi: 10.25140/2411-5363-2019-1(15)-145-151 [in Ukrainian].

18. Filipishyna L., Kostyk Ye., Dzveliuk M. Publichne upravlinnia u sferi informatsiinoi bezpeky (podolannia suchasnykh zahroz). *Aktualni pytannia u suchasnii nautsi.* 2023. № 5. S. 196-205. doi: https://doi.org/10.52058/2786-6300-2023-5(11)-196-205 [in Ukrainian].

19. Shopina I. Informatsiina bezpeka tsyfrovoi transformatsii. *Naukovyi visnyk Lvivskoho derzhavnoho universytetu vnutrishnikh sprav.* 2023. Vyp. 1. S.

28-35. URL: https://dspace.lvduvs.edu.ua/handle/1234567890/5636 [in Ukrainian].

20. Kramer A. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences of the United States of America.* 2014. 111 (24). P. 8788-8790. doi: 10.1073/pnas.1320040111.