

Політичні науки

УДК 351.746.1(477)«364» +930

Білоус Ліна Василівна

кандидат політичних наук, доцент,

доцент кафедри суспільних наук

Івано-Франківський національний технічний університет нафти і газу

Bilous Lina

Candidate of Political Science, Associate Professor,

Associate Professor of the Department of Social Sciences

Ivano-Frankivsk National Technical University of Oil and Gas

ORCID: 0000-0002-1580-8745

**ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ ВОЄННОГО
СТАНУ: ІСТОРИОГРАФІЯ ПРОБЛЕМИ
INFORMATION SECURITY OF UKRAINE UNDER MARTIAL LAW:
HISTORIOGRAPHY OF THE ISSUE**

Анотація. Вступ. В структурі національної безпеки у змістовому плані розрізняється, окрім інших, її інформаційна складова. Значущість останньої у забезпеченні національної безпеки України відображається численними нормативно-правовими документами нашої держави, насамперед, Конституцією, яка відносить інформаційну безпеку до таких найважливіших функцій держави, як захист суверенітету і територіальної цілісності. А прийнята в умовах російської воєнної агресії, яка супроводжується потужним інформаційним впливом на українське суспільство, Стратегія інформаційної безпеки дає її базове тлумачення, визначає глобальні та національні виклики й загрози, стратегічні цілі та напрями реалізації.

Проблема інформаційної захищеності українського суспільства помітно загострилася в умовах повномасштабної війни РФ проти нашої держави з лютого 2022 року. Логічно, що реально існуючий стан справ із забезпеченням інформаційної безпеки в Україні актуалізує численні наукові дослідження різних аспектів зазначеної проблеми. В системі сучасної соціогуманітаристики її дослідженню присвятили свої праці велика кількість вітчизняних науковців, серед яких: І. Ільницька, Н. Авер'янова та Т. Воропаєва, Ю. Лісовська, І. Боднар, О. Гуровський, І. Валюшко, Е. Домбровська та О. Левченко, О. Панченко та Л. Панченко, В. Ліпкан, Д. Максименко та В. Желіховський, ін. При цьому зауважимо, що їх наукові розробки торкалися проблем інформаційної безпеки періоду до повномасштабного вторгнення Росії в Україну.

Мета. Огляд найбільш продуктивних, на наш погляд, праць вітчизняних науковців з дослідження проблеми інформаційної безпеки України в умовах воєнного стану та визначення ключових аспектів цих досліджень.

Матеріали і методи. Матеріалами виступили наукові публікації українських авторів, а також базові нормативно-правові документи Української держави з питань національної та інформаційної безпеки. У процесі дослідження були використані загальнонаукові методи.

Результати. Визначено ключові аспекти досліджень вітчизняними науковцями проблеми інформаційної безпеки України в умовах воєнного стану.

Перспективи. Подальші дослідження можуть бути спрямовані на періодичний аналіз та систематизацію дослідницької бази, що динамічно розвиватиметься, з проблем інформаційної безпеки України.

Ключові слова: *інформаційна безпека України, воєнний стан, вітчизняні вчені, наукові праці, аспекти досліджень.*

Summary. *Introduction. Within the structure of national security, its informational component stands out in terms of content, alongside the other components. The significance of the informational one in ensuring Ukraine's national security is reflected in numerous regulatory and legal documents of our state, primarily the Constitution, which includes information security among the most important functions of the state, such as the protection of sovereignty and territorial integrity. The Information Security Strategy, adopted under the conditions of russian military aggression, which is accompanied by powerful informational influence on Ukrainian society, provides a basic interpretation of information security, defines global and national challenges and threats, as well as strategic goals and implementation directions.*

The problem of information security of Ukrainian society has significantly escalated in the context of russia's full-scale war against our state since February 2022. It is logical that the current state of affairs regarding information security provision in Ukraine has prompted numerous scientific studies on various aspects of this issue. In the field of contemporary social sciences and humanities, many domestic scholars have dedicated their work to its study, including: I. Ilnytska, N. Averianova, T. Voropaieva, Yu. Lisovska, I. Bodnar, O. Hurivskyi, I. Valiushko, E. Dombrovska, O. Levchenko, O. Panchenko, L. Panchenko, V. Lipkan, D. Maksymenko, V. Zhelikhovskyi, and others. It should be noted, however, that their scientific work primarily addressed the issue of information security before russia's full-scale invasion of Ukraine.

Objective. *To review the most productive, in our opinion, works of domestic scholars on the study of information security of Ukraine under martial law and to identify the key aspects of these studies.*

Materials and Methods. *The materials include scientific publications by Ukrainian authors, as well as basic regulatory and legal documents of the Ukrainian state on national and information security matters. General scientific methods were used in the course of the research.*

Results. The key aspects of research conducted by domestic scientists on the issue of Ukraine's information security in the context of martial law have been identified.

Perspectives. Further research may be aimed at periodic analysis and systematization of the research base, which will develop dynamically, on the issues of Ukraine's information security.

Key words: *information security of Ukraine, martial law, domestic scholars, scientific works, research aspects.*

Постановка проблеми. У змістовому плані національної безпеки як стану держави, який дає їй можливість зберігати свою цілісність і виступати самостійним суб’єктом системи міжнародних відносин, розрізняють, зокрема, інформаційну складову. Про важливість останньої для забезпечення національної безпеки Української держави свідчить вагомий перелік прийнятих, починаючи з 90-х років минулого століття, в її сфері нормативно-правових документів [1]. Основним правовим базисом нормотворчості в інформаційній сфері виступає Конституція, яка гарантує кожному право вільно збирати, зберігати, використовувати і поширювати інформацію (ст. 34) та відносить інформаційну безпеку до низки найважливіших функцій держави, таких, як захист суверенітету і територіальної цілісності (ст. 17) [2].

Російська воєнна агресія проти України показала свій потужний інформаційний супровід, що спричинило трансформацію національного інформаційного законодавства. З метою забезпечення інформаційної безпеки в Україні було прийнято, крім усього іншого, концептуальний документ – Стратегію інформаційної безпеки (2021), яка визначає глобальні й національні виклики та загрози інформаційній безпеці, стратегічні цілі та напрями реалізації Стратегії. Остання тлумачить інформаційну безпеку як «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 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» [3].

Реально існуюча в умовах російсько-української війни проблема інформаційної безпеки, яка помітно загострилася з повномасштабним російським вторгненням, а також зазначені в нормативно-правових документах базові засади її розуміння обумовлюють численні наукові розвідки різних аспектів вказаної проблеми. Дотичними до останньої стануть також, сподіваємось, і напрацювання викладачів кафедри суспільних наук ІФНТУНГ в рамках нещодавно затвердженої теми держбюджетної науково-дослідної роботи «Людський потенціал: соціально-гуманітарні виміри національної безпеки».

Аналіз останніх досліджень і публікацій. Проблема інформаційної безпеки України є доволі актуальною і займає важливе місце в системі сучасної соціогуманітаристики. Вона знайшла своє відображення в працях великої кількості вітчизняних науковців. У коло даної проблематики входять, зокрема, дослідження: теоретичних підходів до визначення сутності поняття «інформаційна безпека», видів реальних і потенційних інформаційних загроз для медіапростору України, надання практичних рекомендацій щодо вдосконалення державної інформаційної політики та створення ефективної системи інформаційної безпеки України [4]; соціогуманітарного виміру інформаційної безпеки, тобто інформаційно-

психологічної безпеки українського суспільства, сутність якої полягає в захищеності від заподіяння шкоди як національних інформаційних ресурсів, так і психічного здоров'я людини й суспільства [5]; щодо формування теоретико-правових засад адміністративно-правового забезпечення інформаційної безпеки в Україні [6]; основних напрямів державної інформаційної політики із забезпечення захисту національного інформаційного простору та гарантування інформаційної безпеки [7]; основних законодавчих та інших нормативно-правових актів України в інформаційній сфері, прийнятих внаслідок російської збройної агресії [1]; механізмів забезпечення інформаційної безпеки як складової державної безпеки [8]; окремих питань інформаційної безпеки суб'єктів господарювання, зокрема, корпорацій [9]; взаємозв'язку інформаційної безпеки та інформаційної культури [10]; національних інтересів в інформаційній сфері, засад інформаційної безпеки Євросоюзу та адаптації стандартів останнього до українського інформаційного законодавства [11]; російсько-української війни та інформаційної ідентичності в медіа 2014–2022 років [12] тощо.

Зауважимо, що усі ці дослідження стосувалися аналізу інформаційної безпеки до початку великої війни росії проти нашої країни. Наукові напрацювання вітчизняних авторів з проблем інформаційної безпеки України час від часу актуалізує їх огляд, систематизацію та узагальнення. Певна річ, що тією чи іншою мірою дослідницькі кроки в історіографії конкретно визначеного аспекту (-ів) проблеми інформаційної безпеки здійснюються кожним науковцем. Але це зазвичай виступає як один з необхідних елементів структури дослідження, а не його ціль.

Метою статті є огляд найбільш продуктивних, на нашу думку, праць вітчизняних науковців з дослідження проблеми інформаційної безпеки України в умовах воєнного стану та визначення ключових аспектів цих досліджень.

Виклад основного матеріалу. У науковій розвідці М. Шевчука головна увага приділяється аналізу генези поняття «інформаційна безпека» як складової національної безпеки. Висвітливши історичні трактування сутності феномену інформаційної безпеки, розуміння його деякими вітчизняними науковцями та зауваживши, що чинне українське законодавство не дає розгорнутого тлумачення цього поняття, автор пропонує власне визначення інформаційної безпеки як «стійкого стану інформаційної сфери, що забезпечує її цілісність і захищеність об'єктів за наявності негативних внутрішніх і зовнішніх впливів, заснований на усвідомленні людиною своїх цінностей, потреб (життєво важливих інтересів) і цілей розвитку» [13, с. 138]. На думку дослідника, філософський зміст запропонованої дефініції складають онтологічна (фіксує ситуацію управління ризиками, метою якого є забезпечення цілісності об'єкта та стабільного стану інформаційного середовища), антропологічна (розкриває безпеку суб'єктів інформаційної взаємодії) та аксіологічна (відображає цінності та цілі, які визначають інформаційні потреби людини) складові. Учений є прибічником комплексного підходу до розуміння інформаційної безпеки як одночасно стану і процесу. Якщо перший забезпечує самозбереження, сталий і прогресивний розвиток інформаційної сфери (інфраструктури, простору, ресурсів, процесів та їх суб'єктів тощо), то другий – це перманентний процес діяльності компетентних державних органів, спрямований на запобігання та протидію загрозам інформаційної сфери, вжиття активних заходів інформаційним впливам, а також сукупність умов для цієї діяльності [13, с. 138].

Аналогічне питання визначення, аналізу генези поняття інформаційної безпеки в науковій сфері та важливості забезпечення захисту інформаційного простору України в умовах російсько-українського воєнно-політичного конфлікту висвітлює Я. Лелет [14].

Дослідники Л. Смотрич та Л. Браїлко розглядають інформаційну безпеку в умовах воєнного стану через призму висвітлення типових загроз інформаційній безпеці ЗСУ та пріоритетних напрямів забезпечення безпеки. До загроз вони відносять: напруженість і дестабілізацію суспільно-політичної ситуації в місцях дислокації Збройних Сил, викликану штучно «нагрітою» атмосферою, провокуванням кадрових конфліктів з місцевим населенням; фальсифікацію фактів військової історії; поширення радикального ісламізму; технічні загрози інформаційного характеру, які стосуються як функціонування інформаційних систем, що використовуються у військах, так і збереження конфіденційної інформації, що передається військовими каналами зв'язку; недостатню розвиненість законодавчої бази щодо захисту інформації та протидії новим загрозам (тут автори зауважують, що з моменту оголошення воєнного стану в Україні прийнято зміни до нормативно-правових актів з урахуванням реалій війни); застосування противником нових видів інформаційної зброї, частина з яких спрямована на виведення з ладу інформаційних систем, а частина – на прямий психологічний вплив на особовий склад (використання ультразвуку, електромагнітних полів, мікрохвиль різної природи, а також медичних та хімічних засобів, які можуть дезорієнтувати поведінку військовослужбовців); наявність соціальних мереж, за допомогою яких військові можуть випадково оприлюднити важливу інформацію тощо.

Науковці пропонують й власне бачення основних напрямів захисту інформаційної безпеки відповідно до вказаних загроз. Ними є: цілеспрямована психолого-просвітницька робота з особовим складом; налагодження контактів з регіональною владою з метою недопущення провокаційної роботи медіа та інших джерел поширення інформаційних атак; підвищення рівня безпеки автоматизованих систем управління та навчання персоналу необхідним вимогам захисту інформації; своєчасне виявлення та усунення загроз, пов'язаних з діяльністю різноманітних

соціальних мереж; розробка інформаційної зброї не тільки для відображення загроз, а й для їх передбачення тощо [15].

В аспекті забезпечення інформаційних прав та свобод висвітлює інформаційну безпеку України в умовах воєнного стану дослідниця І. Котерлін. Вона звертає увагу на необхідність забезпечення балансу між реалізацією національної безпеки держави та прагненнями українського суспільства зберегти її правовий характер. Науковиця аналізує нормативно-правові документи (Конституцію, Стратегію національної безпеки, Стратегію інформаційної безпеки, ін.) з точки зору їх спрямованості на захист державного суверенітету, територіальної цілісності, демократичного конституційного ладу тощо, загалом того, що сприяє забезпеченню конституційних прав і свобод людини. Разом з тим зауважує, що останні часто неможливо забезпечити через втрату юрисдикційних спроможностей у частині областей України та внаслідок інших безпосередніх загроз, направлених проти існування самої Української держави та її громадян. Авторка посилається на Указ президента України «Про введення воєнного стану в Україні», де вказується на можливість обмеження конституційних прав і свобод людини і громадянина, передбачених статтями 30–34, 38, 39, 41–44, 53 Конституції України, вагому частину яких становлять інформаційні права і свободи. Дослідниця вважає, що у воєнний час перевага інтересів держави означає можливість збереження основоположних прав багатьох людей через забезпечення життєздатності самої держави, тобто захист інформаційної безпеки держави є пріоритетним, оскільки від нього залежить безпека суспільства і людини. А завершення воєнного стану автоматично активує тимчасово призупинену дію вищевказаних норм [16].

У тезах доповіді на міжнародній науково-практичній конференції дослідники І. Р. Шинкаренко та І. І. Шинкаренко зазначили, що формування інформаційної безпеки в умовах війни є комплексом політичної, правової та

технічної діяльності уповноважених державних органів, направленої на захист громадян, суспільства і держави. Акцентуючи на правовій складовій інформаційної безпеки, автори підкреслили значущість для її забезпечення таких базових документів, як Стратегія інформаційної безпеки, Указ президента України щодо введення в дію Рішення РНБОУ «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» (2022), а також проаналізували важливість прийнятих змін до деяких нормативно-правових актів, які торкаються врегулювання: питань інформаційних правовідносин щодо заборони поширювати певну інформацію, яка має суспільно небезпечний характер; деяких аспектів технічного фіксування інформації; процесуальних дій щодо вилучення інформації; питань про кримінальну відповідальність за незаконну фото- та відео-зйомку переміщення ЗСУ та міжнародної військової допомоги під час воєнного стану; спрощення проведення слідчих дій та тимчасових доступів до речей і документів [17].

У науковій розвідці І. Залєвської та Г. Удренас інформаційна безпека України досліджується через призму аналізу можливостей реалізації семи цілей, зазначених в Стратегії інформаційної безпеки, за умов воєнного стану. Так, головним інструментом для реалізації першої цілі – протидії дезінформації та інформаційним операціям (насамперед держави-агресора), – має бути, на думку авторів, правда, яку потрібно доносити як до внутрішньої, так і до закордонної аудиторії, а також медіакультура та медіаграмотність населення.

Друга ціль – забезпечення всебічного розвитку української культури та утвердження української громадянської ідентичності – може бути здійснена, як вважають автори публікації, через культурну експансію України, щоб спрямувати увагу світу до української культури і мистецтва та сконсолідувати міжнародну спільноту у спротиві російській агресії.

В умовах інформаційної війни, в ході якої поширюється безліч фейків та ботів, надзвичайно важливим, на переконання учених, є реалізація такої

цілі Стратегії, як підвищення рівня медіакультури та медіаграмотності суспільства. Допомогти людям адекватно поводитися в інформаційному середовищі можуть органи влади та структури громадянського суспільства завдяки проведенню постійної роз’яснювальної роботи через медіа.

Четверта ціль Стратегії – забезпечення інформаційних прав особи, захисту прав журналістів – особливо вагома в умовах великої війни, оскільки саме журналісти добувають і несуть у маси правду про реалії війни, нерідко піддаючись з боку російського агресора обстрілам, погрозам, переслідуванням, захопленням телевеж, хакерським атакам на сайти українських медіа, вимкненням українського мовлення на тимчасово окупованих територіях тощо. Враховуючи, що одним з основних прав людини є доступ до інформації, українська влада, як вважають дослідники, має робити все для того, щоб це право ніколи не було порушено.

Забезпечити реалізацію наступної цілі Стратегії інформаційної безпеки – інформаційну реінтеграцію громадян України, які проживають на тимчасово окупованих територіях та прилеглих до них територіях України, до загальноукраїнського інформаційного простору, – було, на думку науковців, складним і до повномасштабного нападу росії на Україну. Ще складнішим це завдання є в умовах воєнного стану, адже агресор робить все, щоб розірвати інформаційні та культурні зв’язки з Україною тих українців, які там проживають. Тому найвірогідніший варіант реалізації цієї цілі дослідники пов’язують з перемогою України та великою роллю у цьому процесі гуманітарної освіти.

Шоста ціль Стратегії – створення ефективної системи стратегічних комунікацій, яка передбачає гарантування ефективної інформаційної взаємодії між органами державної влади, місцевого самоврядування та суспільством з питань кризових ситуацій; зміцнення позитивного іміджу України. Автори дослідження вважають, що перша частина завдання в умовах війни здійснюється на високому рівні. Що ж до формування іміджу

України – це зона відповідальності зовнішніх комунікацій. В будь-якому разі, зміцнення як внутрішнього, так і зовнішнього іміджу нашої держави необхідне, на переконання дослідників, тому, що він багато в чому впливає на економічну та культурну перспективу розвитку країни.

Сьома ціль Стратегії інформаційної безпеки – це розвиток інформаційного суспільства та підвищення рівня культури діалогу. Як вважають учені, одним із найістотніших об'єктів безпеки в оборонній сфері сьогодні є інформаційні ресурси та інформаційна структура оборонного потенціалу країни, які можуть виявитися дуже вразливими з погляду впливу інформаційної зброї як у військовий, так і в мирний час. Тому рівень забезпечення військової сфери засобами захисту від застосування інформаційно ємних технологічних досягнень прямо впливає на рівень національної безпеки держави.

Володіння інформаційними ресурсами та їх захист у військовій сфері стали, як підкреслюють дослідники, таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт. Відповідно, виграш України в інформаційному протиборстві під час війни з росією сприятиме, на переконання науковців, досягненню її стратегічних цілей. Висновуючи своє дослідження, автори зазначають, що здійснений ними аналіз ходу реалізації цілей Стратегії показав, що цей процес не зупиняється, незважаючи на труднощі воєнного часу [18].

Науковець А. Ключко метою свого дослідження означив аналіз системи забезпечення інформаційної безпеки в сучасній Україні через висвітлення рівнів (законодавчого та адміністративного) механізму захисту інформаційної безпеки; переліку загроз інформаційній безпеці країни; питання потреби вивчення досвіду інших країн (США, Великої Британії, Ізраїлю, ФРН, РФ, Китаю) для посилення протидії інформаційній війні росії проти України; основних заходів щодо забезпечення інформаційної безпеки України у зовнішньополітичній сфері.

Головним стратегічним завданням інформаційної безпеки України дослідник називає створення потужного національного інформаційного простору як того аспекту, що засвідчує присутність країни на світовій інформаційній арені, а також – системи протистояння будь-якій інформаційній загрозі та оборони власних інформаційних ресурсів, середовища та інфраструктурної складової країни. В механізмі захисту інформаційної безпеки автор розрізняє два рівні – законодавчий та адміністративний. Найважливішим на законодавчому рівні вважає створення механізму, що дозволяє узгодити процес розробки законів з реаліями та прогресом інформаційних технологій. Головною метою адміністративного рівня називає сформування програми робіт в галузі інформаційної безпеки та забезпечення її виконання, виділяючи для цього необхідні ресурси і контролюючи стан справ. Запорукою ж створення надійної системи охорони інформації А. Ключко вважає зміцнення самої Української держави та її органів, відповідальних за забезпечення інформаційної безпеки в країні [19].

Мета наукової публікації Т. Амро полягає в аналізі взаємозв'язку між системами забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану; визначення методів і можливостей для ефективного забезпечення інформаційної безпеки в цих умовах. Задля цього автор, зокрема, акцентував на ролі публічного управління в забезпеченні інформаційної безпеки в умовах російсько-української війни, яка полягає в наступному: контролі за виконанням законодавства у сфері інформаційної безпеки та забезпеченні дотримання прав і свобод громадян, а також розробці і впровадженні стратегії і програми щодо захисту критично важливої інформації; моніторингу інформаційних потоків, поширенні достовірної інформації про ситуацію на фронті та в країні в цілому; забезпеченні ефективної комунікації між зацікавленими сторонами задля уникнення спотворення та недостовірної інформації; забезпеченні захисту

інформації від хакерських атак та кібернападів, запобіганні поширенню фейків та дезінформації.

До методів і можливостей забезпечення інформаційної безпеки дослідник відносить такі, як: забезпечення кібербезпеки і захисту інформації; сприяння інформаційній війні; забезпечення фізичної безпеки інформації; громадський контроль; неможливість для публічного службовця обмежити доступ до інформації, не пояснивши, чому її оприлюднення завдасть більше шкоди, ніж принесе користі; розробка та впровадження спеціальних заходів технічного захисту інформації, які дозволять забезпечувати конфіденційність і цілісність даних; забезпечення ефективної комунікації між державними структурами та військовими підрозділами; використання системи раннього попередження про надходження інформаційної загрози; використання інформаційних технологій та електронного управління; розвиток системи публічної інформації та масової комунікації; створення ефективної системи моніторингу та аналізу інформації; підвищення медіакультури населення [20].

У науковій розвідці Л. Мазуренко аналізуються виклики і загрози (чутки, плітки, фейки) інформаційній безпеці України; головні шляхи поширення недостовірної інформації (соціальні мережі, підроблені акаунти відомих людей, телерадіомовні канали, особисті повідомлення в різноманітних месенджерах тощо); розкриваються основні механізми протидії неправдивій інформації в умовах війни (формування медіаграмотності населення через критичне мислення, орієнтування в медіа, споживання медіа та дизайн медіа; висвітлення об'єктивної інформації через державні інтернет-видання, медіа, електронне врядування; встановлення відповідальності за поширення неправдивих новин серед населення; контроль фейкових акаунтів та нейтралізація фейків срецпідрозділами кіберполіції); диференціюються такі складові

інформаційної безпеки, як інформаційно-технічний (додержання закону та правопорядку в кіберпросторі) та інформаційно-психологічний (захист психічного стану суспільства та держави від деструктивного інформаційного впливу); визначаються та охарактеризовуються головні напрями підвищення інформаційної безпеки як складової національної безпеки України. До останніх дослідниць відноситься: стратегічне стримування та припинення бойових дій та військових конфліктів; поліпшення системи забезпечення інформаційної безпеки ЗСУ, інших військових формувань; прогнозування, виявлення та оцінка загроз, включаючи загрози для Збройних Сил у сфері інформації.

Визнаючи демонстрацію нинішньою війною інформації як зброї масового ураження, науковиця переконана в необхідності синхронізованих дій структур держави і громадянського суспільства з метою забезпечення інформаційної безпеки України, а також залучення до цього процесу міжнародних організацій, інституцій та загалом міжнародної спільноти. В основу механізму забезпечення інформаційної безпеки важливо покласти технічну (створення належної технічної бази функціонування безпеки), політичну (направленість державної політики на її забезпечення) та правову (оформлення усіх заходів інформаційної безпеки якісними нормативно-правовими актами) складові [21].

Науковиці І. Лопатченко, А. Помаза-Пономаренко та Ю. Батир досліджують особливості державного регулювання інформаційної безпеки в умовах воєнного стану головним чином через аналіз діяльності створеного за рішенням РНБОУ Центру протидії дезінформації (2021). Авторки статті висвітлюють основні завдання Центру, його пріоритети (оперативне інформування населення; розкриття дезінформації та маніпуляцій; забезпечення інформаційної безпеки; боротьба з інформаційним тероризмом), розроблені фахівцями Центру конкретні поради та рекомендації як зруйнувати так звану інформаційну бульбашку (стан

інтелектуальної ізоляції людини). Як і згадана нами вище Л. Мазуренко, ці дослідниці також вважають, що ефективна система інформаційної безпеки має базуватися на узгоджених діях державних структур та громадянського суспільства і включати в себе технічну, політичну, правову компоненти [22].

Правові механізми забезпечення інформаційної безпеки в Україні в умовах повномасштабної війни розглядаються в статті О. Скочиляс-Павлів. Дослідниця пропонує своє розуміння інформаційної безпеки як «стану захищеності інформаційних ресурсів та інформаційних систем, який забезпечує їхню конфіденційність, цілісність, доступність і надійність, а також захищеність від несанкціонованого доступу, розголошення, модифікації, знищення та інших форм зловживань, що можуть призвести до порушення національної безпеки, економічної стабільності та суспільного порядку» [23, с. 3]. При цьому головними принципами інформаційної безпеки держави в цілому, окремих органів та приватних підприємств називає, як і багато інших науковців, конфіденційність (дані мають бути доступні лише тим, хто має авторизований доступ), цілісність (інформація має бути недоторканою, повною і точною) та доступність (мережа, система, необхідні пристрої готові до використання за призначенням уповноваженим персоналом), а основними компонентами механізму забезпечення інформаційної безпеки – технічний, політичний та правовий. Авторка вважає, що тільки завдяки комплексному підходу, який включає підвищення рівня кібербезпеки, освіти та обізнаність громадян, розвиток правової бази, міжнародне співробітництво і впровадження відповідних кроків можна домогтися забезпечення ефективної інформаційної безпеки, особливо в умовах війни [23].

Висновки та перспективи подальших досліджень. Здійснений аналіз історіографії проблеми інформаційної безпеки України в умовах воєнного стану дозволив визначити такі основні, на нашу думку, аспекти досліджень, які стосуються висвітлення:

- тлумачень поняття інформаційної безпеки історично, сучасними науковцями, українськими нормативно-правовими актами; інформаційно-технічної та інформаційно-психологічної складових інформаційної безпеки; технічного, політичного і правового аспектів механізму її забезпечення;
- типових загроз і викликів інформаційній безпеці ЗСУ, суспільства в цілому; пріоритетних напрямів захисту безпеки відповідно до цих загроз; вивчення досвіду інших країн для посилення протидії інформаційній війні росії проти України;
- проблеми забезпечення балансу інформаційних прав та свобод і національної безпеки держави;
- можливостей реалізації цілей Стратегії інформаційної безпеки;
- взаємозв'язку між системами забезпечення інформаційної безпеки та публічного управління, методів і можливостей для ефективного реалізації інформаційної безпеки;
- законодавчого та адміністративного рівнів механізму захисту інформаційної безпеки; особливостей її державного регулювання (на прикладі діяльності Центру протидії дезінформації).

Щодо перспектив подальших досліджень зазначимо, що, оскільки науковий інтерес до проблеми інформаційної безпеки як невід'ємної складової безпеки національної динамічно поповнюватиме дослідницьку базу, це періодично потребуватиме аналізу та систематизації.

Література

1. Валюшко І. О. Інформаційна безпека України: трансформація законодавства після російського вторгнення. URL: <https://ir.kneu.edu.ua/server/api/core/bitstreams/4139c437-5fb8-450f-9eb1-8c25fbe1b9a3/content> (дата звернення: 10.12.2024).

2. Конституція України. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text> (дата звернення: 10.12.2024).

3. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 10.12.2024).

4. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Політичні науки*. 2016. Vol. 2, No. 1. С. 27–32. URL: <https://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/4352/ilnicka0.pdf> (дата звернення: 10.12.2024).

5. Авер'янова Н. М., Воропаєва Т. С. Інформаційна безпека України: соціально-філософські аспекти. *Філософські науки*. 2020. № 10 (86). С. 297–303. URL: <https://molodyivchenyi.ua/index.php/journal/article/view/319/308> (дата звернення: 10.12.2024).

6. Лісовська Ю. П. Адміністративно-правове забезпечення інформаційної безпеки в Україні: автореф. дис. на здобуття наук. ступеня канд. юрид. наук.: спец.: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. К., 2017. 19 с. URL: https://maup.com.ua/assets/files/avtoreferat_lisovska.pdf (дата звернення: 10.12.2024).

7. Боднар І. Р. Інформаційна безпека як основа національної безпеки. *Механізм регулювання економіки*. 2014. № 1. С. 68–75. URL: <https://core.ac.uk/download/pdf/141443493.pdf> (дата звернення: 10.12.2024).

8. Домбровська С. М. Механізми забезпечення інформаційної безпеки як складової державної безпеки України. *Теорія та практика державного управління*. 2015. Вип. 1. С. 203–207.

9. Нашинець-Наумова А. Ю. Інформаційна безпека: питання правового регулювання: монографія. К.: Видавничий дім «Гельветика», 2017. 168 с.

10. Панченко О. А., Панченко Л. В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. 2015. № 2(46). С. 32–38.

11. Ліпкан В. А., Максименко Ю. Є., Желіховський В. М. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.

12. Логвинюк Т. Інформаційна безпека в умовах геополітичного виклику: аналіз російсько-української війни та інформаційної ідентичності в ЗМІ 2014–2022 рр. *Український літопис*. 2024. № 3. С. 51–57. <https://doi.org/10.31470/2786-8583-2024-3-51-57>.

13. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Том 2, № 78. С. 134–139. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/2800582> (дата звернення 10.12.2024).

14. Лелет Я. Генеза інформаційної безпеки в умовах воєнно-політичного конфлікту. *Вісник Прикарпатського університету. Серія: Політологія*. 2024. № 19. С. 98–104. <https://journals.pnu.if.ua/index.php/politology/issue/view/21> (дата звернення: 10.12.2024).

15. Смотрич Д. В., Браїлко Л. Інформаційна безпека в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Том 2, № 77. С. 121–127. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/284104/278250> (дата звернення: 10.12.2024).

16. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. *Актуальні проблеми*

вітчизняної юриспруденції. 2022. № 1. С. 150–155. URL: http://apnl.dnu.in.ua/1_2022/25.pdf (дата звернення: 10.12.2024).

17. Шинкаренко І. Р., Шинкаренко І. І. Сучасні проблеми правового, економічного та соціального розвитку держави: тези доп. XI міжнар. наук.-практ. конф. (м. Вінниця, 9 груд. 2022 р.). МВС України, Харків. нац. ун-т внутр. справ. Наук. парк «Наука та безпека». Вінниця, 2022. С. 139–140. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/45394d87-8cc7-451e-9f1c-1fbfedf2d7a4/content> (дата звернення: 10.12.2024).

18. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах російської військової агресії. *Південноукраїнський правничий часопис*. 2022. № 1–2. С. 20–26. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/1e9150a5-fe34-42b9-9f26-582b2a89c1ef/content> (дата звернення: 10.12.2024).

19. Ключко А. Забезпечення інформаційної безпеки в умовах сучасного суспільства. *Наукові праці Міжрегіональної Академії управління персоналом. Політичні науки та публічне управління*. 2022. № 3(63). С. 38–43. URL: <https://journals.maup.com.ua/index.php/political/issue/view/230/247> (дата звернення: 10.12.2024).

20. Амро Т. Взаємозв’язок систем забезпечення інформаційної безпеки та публічного управління в умовах воєнного стану: методи та можливості. *Публічне урядування: збірник*. 2022. № 5(33). С. 83–88. URL: <https://journals.maup.com.ua/index.php/public-management/issue/view/251/270> (дата звернення: 10.12.2024).

21. Мазуренко Л. І. Інформаційна безпека в умовах російсько-української війни: виклики та загрози. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Питання політології»*. 2022. Вип. 42. С. 50–57. <https://doi.org/10.26565/2220-8089-2022-42-08>.

22. Лопатченко І. М., Помаза-Пономаренко А. Л., Батир Ю. Г. Державне регулювання у сфері інформаційної безпеки України в умовах

воєнного стану. С. 14–24. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/20308/1/2Lopatchenko.pdf> (дата звернення: 10.12.2024).

23. Сkochиляс-Павлів О. Правові механізми забезпечення інформаційної безпеки в Україні. *Вісник Національного університету «Львівська політехніка»*. Серія: «Юридичні науки». 2024. Вип. 11, № 2(42). С. 151–158. URL: <https://science.lpnu.ua/uk/law/vsi-vypusky/volume-11-number-2-42-2024/pravovi-mehanizmy-zabezpechennya-informaciynoi-bezpeky> (дата звернення: 10.12.2024).

References

1. Valiushko I. O. Information Security of Ukraine: Transformation of Legislation after the russian Invasion. URL: <https://ir.kneu.edu.ua/server/api/core/bitstreams/4139c437-5fb8-450f-9eb1-8c25fbe1b9a3/content> [in Ukrainian].

2. Constitution of Ukraine. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96%D0%B2%D1%80#Text> [in Ukrainian].

3. About the Decision of the National Security and Defense Council of Ukraine from October 15, 2021, «About the Strategy of Information Security»: The Decree of the President of Ukraine. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> [in Ukrainian].

4. Ilnytska U. Information Security of Ukraine: Current Challenges, Threats, and Mechanisms for Counteracting Negative Information and Psychological Impacts. *Political Science*. 2016. Vol. 2, No. 1. pp. 27–32. URL: <https://science.lpnu.ua/sites/default/files/journalpaper/2017/jun/4352/ilnicka0.pdf> [in Ukrainian].

5. Averianova N. M., Voropaieva T. S. Information Security of Ukraine: Socio-philosophical Aspects. *Philosophical Science*. 2020. No. 10 (86). pp. 297–

303. URL: <https://molodyivchenyi.ua/index.php/journal/article/view/319/308> [in Ukrainian].

6. Lisovska Yu. P. Administrative and Legal Support for Information Security in Ukraine: Abstract of Dissertation for the Scientific Degree of Candidate of Legal Sciences: Specialty: 12.00.07 – Administrative Law and Procedure; Financial Law; Information Law. Kyiv, 2017. 19 p. URL: https://maup.com.ua/assets/files/avtoreferat_lisovska.pdf [in Ukrainian].

7. Bodnar I. R. Information Security as a Basis of National Security. *Mechanism of Economic Regulation*. 2014. No. 1. pp. 68–75. URL: <https://core.ac.uk/download/pdf/141443493.pdf> [in Ukrainian].

8. Dombrovska S. M. Mechanisms for Ensuring Information Security as a Component of State Security of Ukraine. *Theory and Practice of Public Administration*. 2015. Issue 1. pp. 203–207 [in Ukrainian].

9. Nashynets-Naumova A. Yu. Information Security: Issues of Legal Regulation: Monograph. Kyiv: Publishing House «Helvetica», 2017. 168 p. [in Ukrainian].

10. Panchenko O. A., Panchenko L. V. Information Security and Information Culture in the Modern Information Society. *Legal Informatics*. 2015. No. 2(46). pp. 32–38 [in Ukrainian].

11. Lipkan V. A., Maksymenko Yu. Ye., Zhelikhovskiy V. M. Information Security of Ukraine in the Context of European Integration: Textbook. Kyiv: KNT, 2006. 280 p. [in Ukrainian].

12. Lohvyniuk T. Information Security in the Context of the Geopolitical Challenge: Analysis of the russian-Ukrainian War and Information Identity in the Media in 2014–2022. *Ukrainian Chronicle*. 2024. No. 3. pp. 51–57. <https://doi.org/10.31470/2786-8583-2024-3-51-57> [in Ukrainian].

13. Shevchuk M. O. About the Genesis of the Concept of Information Security as a Component of National Security. *Scientific Bulletin of Uzhhorod*

National University. Series: Law. 2023. No. 78, Vol. 2. pp. 134–139. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/2800582> [in Ukrainian].

14. Lelet Ya. The Genesis of Information Security in the Context of Military-Political Conflict. *Bulletin of Precarpathian University. Series: Political Science.* 2024. No. 19. pp. 98–104. URL: <https://journals.pnu.if.ua/index.php/politology/issue/view/21> [in Ukrainian].

15. Smotrych D. V., Brailko L. Information Security Under Martial Law. *Scientific Bulletin of Uzhhorod National University. Series: Law.* 2023. Vol. 2, No. 77. pp. 121–127. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/284104/278250> [in Ukrainian].

16. Koterlin I. B. Information Security Under Martial Law in the Aspect of Ensuring Information Rights and Freedoms. *Current Issues of Domestic Jurisprudence.* 2022. No. 1. pp. 150–155. URL: http://apnl.dnu.in.ua/1_2022/25.pdf [in Ukrainian].

17. Shynkarenko I. R., Shynkarenko I. I. Modern Issues of Legal, Economic, and Social Development of the State: Abstracts of the 11th International Scientific-Practical Conference (Vinnytsia, December 9, 2022). Ministry of Internal Affairs of Ukraine, Kharkiv National University of Internal Affairs, Scientific Park «Science and Security». Vinnytsia, 2022. pp. 139–140. URL: <https://dspace.univd.edu.ua/server/api/core/bitstreams/45394d87-8cc7-451e-9f1c-1fbfedf2d7a4/content> [in Ukrainian].

18. Zalievska I. I., Udrenas H. I. Information Security of Ukraine in the Context of russian Military Aggression. *Southern Ukrainian Law Journal.* 2022. No. 1–2. pp. 20–26. URL: <https://dspace.oduvs.edu.ua/server/api/core/bitstreams/1e9150a5-fe34-42b9-9f26-582b2a89c1ef/content> [in Ukrainian].

19. Klochko A. Ensuring Information Security in Modern Society. *Scientific Works of the Interregional Academy of Personnel Management. Political Science and Public Administration.* 2022. No. 3(63). pp. 38–43. URL:

<https://journals.maup.com.ua/index.php/political/issue/view/230/247> [in Ukrainian].

20. Amro T. The Interrelation of Ensuring Information Security Systems and Public Administration Under Martial Law: Methods and Opportunities. *Public Administration: Collection of Papers*. 2022. No. 5(33). pp. 83–88. URL: <https://journals.maup.com.ua/index.php/public-management/issue/view/251/270> [in Ukrainian].

21. Mazurenko L. I. Information Security Under the Conditions of the russian-Ukrainian War: Challenges and Threats. *The Journal of V. N. Karazin Kharkiv National University. Series: Issues of Political Science*. 2022. Issue 42. pp. 50–57. <https://doi.org/10.26565/2220-8089-2022-42-08> [in Ukrainian].

22. Lopatchenko I. M., Pomaza-Ponomarenko A. L., Batyr Yu. H. State Regulation in the Sphere of Information Security of Ukraine Under Martial Law. *The Journal of NUCZU of Ukraine. Series: Public Administration*. 2024. Issue 1(20). pp. 14–24. URL: <http://repositsc.nuczu.edu.ua/bitstream/123456789/20308/1/2Lopatchenko.pdf> [in Ukrainian].

23. Skochylas-Pavliv O. Legal Mechanisms for Ensuring Information Security in Ukraine. *The Journal of Lviv Polytechnic National University. Series: Legal Sciences*. 2024. Issue 11, No. 2(42). pp. 151–158. URL: <https://science.lpnu.ua/uk/law/vsi-vypusky/volume-11-number-2-42-2024/pravovi-mehanizmy-zabezpechennya-informaciyoi-bezpeky> [in Ukrainian].