

Адміністративне право і процес; фінансове право; інформаційне право
УДК 351.746.1:159.964

Ковалів Мирослав Володимирович

кандидат юридичних наук, професор

Львівський державний університет внутрішніх справ

Kovaliv Myroslav

PhD in Law, Professor

Lviv State University of Internal Affairs

ORCID: 0000-0002-9730-8401

Скриньковський Руслан Миколайович

кандидат економічних наук, професор

Львівський університет бізнесу та права

Skrynkovskyu Ruslan

PhD in Economics, Professor

Lviv University of Business and Law

ORCID: 0000-0002-2180-8055

Петков Сергій Валерійович

доктор юридичних наук, професор

Військовий інститут

Київського національного університету імені Тараса Шевченка

Petkov Sergey

D. Sc. (Law), Professor

Military Institute of

Taras Shevchenko National University of Kyiv

ORCID: 0000-0003-4160-767X

Корецький Олег Павлович

кандидат юридичних наук, адвокат

Koretskyi Oleh

PhD in Law, Lawyer

ORCID: 0009-0000-7463-7731

Чорній Богдан Ігорович

Львівський університет бізнесу та права

Chorniy Bogdan

Lviv University of Business and Law

ORCID: 0009-0000-0440-895X

Микитюк Микола Андрійович

доктор юридичних наук, професор

Інститут Управління державної охорони України

Київського національного університету імені Тараса Шевченка

Mykytiuk Mykola

D. Sc. (Law), Professor

Institute of the Department of the State Protection of Ukraine of

Taras Shevchenko National University of Kyiv

ORCID: 0000-0002-1759-7312

Гудима Віталій Валерійович

кандидат юридичних наук

Управління Служби безпеки України у Львівській області

Hudyma Vitaliy

PhD in Law

Office of the Security Service of Ukraine in Lviv region

ORCID: 0000-0001-6708-3910

**СИСТЕМА ПРАВОВОГО РЕГУЛЮВАННЯ У СФЕРІ
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ**

SYSTEM OF LEGAL REGULATION IN THE FIELD OF ENSURING INFORMATION SECURITY IN UKRAINE

Анотація. У статті розглянуто систему правового регулювання у сфері забезпечення інформаційної безпеки в Україні на основі чинного законодавства України та нормативно-правових актів Європейського Союзу. Об'єктом дослідження є правове регулювання суспільних відносин у сфері забезпечення інформаційної безпеки. Предметом дослідження є структурно-функціональні закономірності системи правового регулювання, закономірні зв'язки між елементами та функціями правового регулювання інформаційної безпеки. Методологічну основу дослідження складають системні та функціональні підходи, логічні методи пізнання: аналіз, синтез, індукція, дедукція, абстрагування, узагальнення, а також приватнонаукові методи. Війна російської федерації проти України викликала необхідність не тільки кардинального оновлення чинного законодавства України, але й переосмислення правового регулювання у сфері забезпечення інформаційної безпеки. Вплив цифрової трансформації та динамічний розвиток інформаційно-комунікаційних технологій свідчать про посилення ролі та значення інформаційної безпеки у системі забезпечення національної безпеки. Особливо важливим є те, що правові акти, які регулюють питання інформаційної безпеки, базуються на комплексному підході до інформаційних загроз, що обумовлено необхідністю стратегічної протидії загрозам та ризикам, спричинених протистоянням в інформаційному просторі. Стратегічне планування забезпечення інформаційної безпеки України в сучасних умовах потребує науково-правового осмислення з позиції права з метою вироблення нових підходів до вирішення пріоритетних завдань, що визначає необхідність удосконалення національної системи правового забезпечення інформаційної безпеки відповідно до стандартів Організації

Північноатлантичного договору (НАТО). У зв'язку з цим зростає значення розвитку правового забезпечення міжнародного співробітництва в галузі інформаційної безпеки.

Ключові слова: безпека, інформація, інформаційна безпека, інформаційні загрози, інформаційно-комунікаційні технології, національні інтереси, державна політика, національна безпека, Україна, НАТО.

Summary. The article reviewed the system of legal regulation in the field of ensuring information security in Ukraine on the basis of the current legislation of Ukraine and regulations of the European Union. The object of the study is the legal regulation of public relations in the field of information security. The subject of the study is the structural and functional patterns of the legal regulation system, the natural connections between the elements and functions of the legal regulation of information security. The methodological basis of the research consists of systemic and functional approaches, logical methods of cognition: analysis, synthesis, induction, deduction, abstraction, generalization, as well as private scientific methods. The war of the Russian Federation against Ukraine has necessitated not only a radical update of the current legislation of Ukraine, but also a rethinking of legal regulation in the field of information security. The influence of digital transformation and the dynamic development of information and communication technologies indicate the strengthening role and importance of information security in the national security system. It is especially important there is that legal acts regulating information security are based on an integrated approach to information threats, which is due to the need to strategically counter threats and risks caused by confrontation in the information space. Strategic planning for ensuring information security in Ukraine in modern conditions requires scientific and legal understanding from the legal perspective in order to develop new approaches to solving priority problems, which determines the need to

improve the national system of legal support for information security in accordance with the standards of the North Atlantic Treaty Organization (NATO). In this regard, the importance of developing legal support for international cooperation in the field of information security is growing.

Key words: *security, information, information security, information threats, information and communication technologies, national interests, state policy, national security, Ukraine, NATO.*

Постановка проблеми. Стан інформаційної безпеки є центральним компонентом політичної, військової, соціально-економічної та інших галузей національної безпеки, є самостійною комплексною сферою національної безпеки, де забезпечується захист інформаційних ресурсів, інформаційних систем і цифрових технологій, національної інформаційної інфраструктури, а також захист інформаційних прав та свобод.

Правове забезпечення інформаційної безпеки є підгалуззю інформаційного права. Однак за обсягом і складністю в умовах високих геополітичних ризиків та викликів загальної цифровізації, його обґрунтовано розглядати як один із елементів інформаційного права, що пронизують всю систему даної галузі та входять складовою частиною до кожного з її інститутів.

Аналіз останніх досліджень і публікацій. За значний вклад у теоретичні розробки правового регулювання забезпечення інформаційної безпеки доцільно відмітити наукові праці: І. Арістової, О. Баранова, В. Дубаса, А. Берлача, П. Діхтієвського, І. Гриценка, С. Єсімова, Л. Кисіль, В. Курила, Є. Курінного, Р. Калюжного, Н. Лесько, О. Малашка, Р. Мельника, В. Настюка, О. Остапенка, А. Селіванова, О. Харитонової, В. Шамрая, І. Шопіної, Я. Шевченко, Ю. Шемчушенка та інших вчених. В умовах воєнного стану, під час російсько-української війни дослідження правового регулювання у сфері забезпечення інформаційної безпеки в

Україні зумовлено метою вдосконалення правового регулювання.

Мета статті. Метою статті є дослідження системи правового регулювання у сфері забезпечення інформаційної безпеки в Україні.

Виклад основного матеріалу дослідження. Система нормативно-правових актів України, які регулюють питання забезпечення інформаційної безпеки особи, суспільства та держави, має досить складну структуру, детерміновану комплексом взаємопов'язаних завдань і заходів, що динамічно ускладнюються в умовах цифрової трансформації. Методологія інформаційної безпеки не заснована на ідеї про поділ права на публічне та приватне, де публічно-правовий і приватноправовий вплив у комплексі дають необхідний регулятивний ефект, що обґрунтовується концепцією єдності правового впливу [1, с. 53].

Ключову роль у правовому регулюванні інформаційної сфери відіграють Закони України «Про інформацію» та «Про захист інформації в інформаційно-комунікаційних системах», які є базовими в інформаційному праві [2; 3]. У цих нормативно-правових актах [2; 3] закріплено основні положення щодо порядку користування інформацією та визначено засади інформаційно-правових відносин у вигляді прав, обов'язків та гарантій усіх учасників цих відносин.

Закон України «Про інформацію» від 02.10.1992 р. № 2657-ХІІ (із змінами) [2] визначає цілі та завдання державної політики щодо правового регулювання питань, віднесених до інформаційного права. У цьому правовому акті закріплені основні положення щодо порядку користування інформацією та визначені засади інформаційно-правових відносин у вигляді прав, обов'язків і гарантій для всіх учасників. Зазначений закон визначає принципи правового регулювання відносин, які виникають у сфері створення, одержання, зберігання, використання, поширення, охорони, захисту інформації (відомостей та/або даних) [2].

Відповідно до Стратегії національної безпеки України, метою

забезпечення інформаційної безпеки є зміцнення суверенітету [4]. Для досягнення зазначеної мети було поставлено низку завдань, серед яких: створення умов для забезпечення цілісності даних з подальшим зберіганням та обробкою інформації серед користувачів інформаційно-комунікаційних мереж; забезпечення належного, відповідного захисту інфраструктури інформаційних технологій.

У Конституції України [5] міститься низка норм, пов'язаних із інформаційною безпекою, які визначають базові ідеї регуляторної та правозастосовної діяльності. Серед норм закріплене право на інформацію, охорону відомостей, які становлять державну таємницю, недоторканість приватного життя, таємницю зв'язку, неприпустимість збору конфіденційної інформації про особу без її згоди. На органах публічної влади лежить обов'язок забезпечення кожній людині можливості ознайомлення з документами та матеріалами, що безпосередньо зачіпають права та свободи [5].

Провідну роль у правовому регулюванні інформаційної безпеки відіграє Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05.07.1994 р. № 80/94-ВР (із змінами) [3]. Цей нормативно-правовий акт регулює порядок захисту інформації з визначенням основних організаційних, правових і технічних заходів, при яких забезпечується конфіденційність, доступність і цілісність даних.

Закон України «Про електронні комунікації» від 16.12.2020 р. № 1089-ІХ (із змінами) [6], з метою забезпечення національних інтересів в інформаційній сфері, регулює особливості поширення інформації в мережі Інтернет, встановлює підстави та порядок обмеження чи закриття доступу до веб-сайтів, які розповсюджують протиправну інформацію [6].

Правове регулювання окремих аспектів забезпечення інформаційної безпеки та захисту певних видів інформації, зокрема, представлене у законодавчих актах, включаючи норми законів: про державну таємницю,

про захист персональних даних, безпеку критичної інфраструктури, електронний підпис, ідентифікації та автентифікації тощо.

Сьогодні відсутній спеціальний закон, який системно формує і регулює комплекс різноманітних суспільних відносин у сфері забезпечення інформаційної безпеки, включаючи питання понятійного апарату, правових принципів, правового статусу основних суб'єктів та основних механізмів, які використовуються, що мають значення для публічної влади.

У законодавстві України існує масив законів, пов'язаних з різними іншими видами безпеки: про біологічну безпеку, про пожежну безпеку (Кодекс цивільного захисту), про техногенну безпеку, про безпеку при експлуатації каналів, трубопроводів та інших гідротехнічних споруд, про використання ядерної енергії та радіаційну безпеку тощо.

Зважаючи на ключову роль забезпечення інформаційної безпеки в умовах інформаційного суспільства та динаміки цифрової трансформації, відсутність спеціального закону, що регулює питання інформаційної безпеки, становить суттєву прогалину у праві.

Нормативно-правові акти державного стратегічного планування вказують на та передбачають зміцнення суверенітету держави в інформаційному середовищі, що має важливе значення у складних умовах цифровізації, особливо під час злочинної війни російської федерації проти України.

У науковій літературі наголошується на значущості Стратегії національної безпеки України для забезпечення гарантій захисту прав і свобод людини та громадянина у сфері безпеки. У нормативно-правовому акті [4] поняття безпеки розглядається у широкому контексті, включаючи державну, економічну, інформаційну, громадську, екологічну та інші види безпеки. У Стратегії національної безпеки України, затвердженої Указом Президента України від 14.09.2020 р. № 392/2020, зазначено, що «людина,

її життя і здоров'я, честь і гідність, недоторканність і безпека – найвища соціальна цінність в Україні. Реалізація цієї норми Конституції України – головна ціль державної політики національної безпеки. ... Україна прагне миру. Мир – запорука розвитку України. Встановлення миру, відновлення суверенітету і територіальної цілісності України у межах її міжнародно визнаного державного кордону – найвищий пріоритет держави» [4].

Законодавець у Стратегії національної безпеки України приділяє особливу увагу інформаційній безпеці. Це зумовлено реалізацією політики інформаційного суверенітету держави та умовами приєднання до єдиного інформаційного простору Європейського Союзу та НАТО (Організації Північноатлантичного договору; англ. NATO – North Atlantic Treaty Organisation). У сфері інформаційно-комунікаційної безпеки необхідно:

- забезпечити кримінально-правовий захист шляхом протидії кримінальним правопорушенням, скоєним у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; мінімізувати протиправні дії проти основ конституційного ладу та безпеки держави; створити ефективні заходи протидії деструктивному інформаційному впливу на людину;

- забезпечити безпеку у сфері безпеки і оборони держави шляхом формування самостійного виду воєнно-інформаційної безпеки;

- вдосконалити та посилити міжнародно-правове співробітництво шляхом співпраці держави з іншими країнами та організаціями з метою підвищення ефективності міжрегіональної взаємодії, уніфікації міжнародних норм, вироблення спільних заходів для запобігання поширенню інформаційних загроз і ризиків, стримування кібератак, забезпечення захисту критично важливих об'єктів, підтримання стабільності та захищеності інформаційного середовища тощо, а також розвивати технологічну і технічну кооперацію з НАТО та ЄС.

Основні напрями державної політики у сфері забезпечення безпеки

України включають широкий спектр питань і аспектів, що стосуються практично всіх сфер життєдіяльності держави. Указами Президента України затверджено: Стратегію інформаційної безпеки [7], Стратегію забезпечення державної безпеки, Стратегію економічної безпеки, Стратегію воєнної безпеки, Стратегію кібербезпеки [8], Доктрину інформаційної безпеки України [9] тощо.

Ключові питання безпеки в інформаційній сфері комплексно відображаються у Стратегії інформаційної безпеки України, затвердженої Указом Президента України від 28.12.2021 р. № 685/2021 [7]. Цей нормативно-правовий акт [7] регулює частину суспільних відносин, завдяки яким цілеспрямовано досягається захищеність держави в інформаційній сфері та визначаються вектори подальшого вдосконалення правових інститутів з метою балансу і захисту інтересів особи, суспільства та держави у цьому середовищі. У даний час з урахуванням суттєвої зміни соціально-економічної та зовнішньополітичної ситуації доцільним є подальший розвиток стратегічного планування у сфері забезпечення інформаційної безпеки.

Слід зазначити, що відповідно до аналізу положень Доктрини інформаційної безпеки України [9] можна виділити особливості національних інтересів: прозорість та транспарентність діяльності держави в інформаційній сфері; гарантія захисту конституційних прав і свобод громадян щодо інформаційної безпеки; взаємне та узгоджене функціонування держави та громадянського суспільства, у тому числі державної політики у сфері утвердження української національної та громадянської ідентичності; забезпечення належного функціонування інформаційної інфраструктури у разі безпосереднього впливу інформаційних загроз у воєнний час та у період стабільної мирної обстановки в країні; стимулювання науково-технічного прогресу та розвитку економічних галузей, що сприяють забезпеченню інформаційної

безпеки; інтеграційна взаємодія з державами-членами НАТО для забезпечення міжнародної інформаційної безпеки та стратегічної стабільності.

Національні інтереси у сфері інформаційної безпеки є спільними орієнтирами для органів публічної влади, на яких покладено функцію управління в галузі нейтралізації інформаційних загроз і конфліктів. Закріплений у документах стратегічного планування перелік національних інтересів є тим правовим фундаментом, на якому стоїть вся система національної безпеки.

На основі положень Закону України «Про національну безпеку України» можна виділити окремі аспекти досліджуваної теми, які відображені у низці підзаконних актів органів публічної влади [10]. Забезпечення інформаційної безпеки держави здійснюється на всіх рівнях органів публічної влади, місцевого самоврядування та недержавними організаціями.

Важливе значення для регулювання окремих напрямів забезпечення інформаційної безпеки та конкретизації норм законів мають постанови та розпорядження Кабінету Міністрів України. Наприклад, Концепція розвитку штучного інтелекту в Україні, яка була схвалена розпорядженням Кабінету Міністрів України [11].

Інституційно-правове забезпечення інформаційної безпеки формується і розвивається на стику галузей інформаційної сфери та сфери забезпечення безпеки. Правове забезпечення інформаційної безпеки концептуально надбудовується на існуючі системи інформаційних правовідносин (базові системи) та забезпечує безпеку їхнього поступального розвитку.

Структурно сукупність регульованих суспільних відносин у сфері організаційно-правового забезпечення інформаційної безпеки характеризується різноманітними об'єктами інформаційної безпеки

(інформаційні ресурси, цифрові дані, інформаційні системи, інформаційно-комунікаційна інфраструктура, цифрові технології); правовим статусом суб'єктів забезпечення інформаційної безпеки; комплексом правових засобів і механізмів, включаючи принципи, методи та заходи забезпечення інформаційної безпеки.

Доцільно застосувати системний підхід під час удосконалення законодавства у сфері інформаційної безпеки, в основі якого має бути відповідна концептуальна модель національної системи інформаційної безпеки.

Роль суб'єктів правового забезпечення інформаційної безпеки, що включають державу, організації, громадські об'єднання та громадян, відрізняється. Ключову роль відіграє держава. Підвищенню ефективності організаційно-правового забезпечення інформаційної безпеки сприятиме наділення певного органу публічної влади спеціальними повноваженнями у сфері інформаційної безпеки.

Потенціал досягнення високого рівня захищеності національних інтересів забезпечуватиметься інтегрованою сукупністю можливостей різних суб'єктів інформаційних відносин, які діють у загальному національному інтересі.

Проблема забезпечення інформаційної безпеки актуалізується разом із збільшенням використання цифрових технологій та підвищенням ймовірності виникнення загроз в умовах цифровізації суспільства. Вирішити цю проблему можна за тісної інтеграційної співпраці між державами, яка передбачає взаємний захист інформації. Налагодження партнерських відносин визначає взаємну відповідальність за інформаційну захищеність кожного з учасників, що в даний час відіграє значну роль при взаємодії України, ЄС та НАТО.

Правове регулювання відносин у сфері національної безпеки визначається потребами врегулювання суспільних відносин, що склалися

між суб'єктами з питань національної безпеки, а також створенням умов для досягнення оптимального рівня безпеки у політичній, правовій, військовій, інформаційній та соціально-економічній сферах.

Зазначені цілі спрямовані на реалізацію конституційних норм, виконання яких на даний час практично неможливе без застосування інформаційно-комунікаційних технологій. Інформаційну безпеку слід розглядати як певне суспільне благо, цінність якого стрімко підвищується за умови узгодженої взаємодії органів публічної влади та громадянського суспільства.

Стан інформаційної безпеки залежить від діяльності законодавця, особи, яка застосовує право, а також від правомірної та відповідальної поведінки фізичних і юридичних осіб. В умовах злочинної війни російської федерації проти України подібна констатація є особливо важливою, оскільки містить заклик до органів публічної влади та суспільства на ефективну протидію агресивній діяльності злочинного російського режиму та запобігання ризикам, пов'язаних з цим.

Мінімізація інформаційного та психологічного впливу на населення під час війни, в тому числі зниження його агітаційно-пропагандистського ефекту, є одним із необхідних способів захисту суспільної безпеки, моральності, здоров'я, прав і законних інтересів громадян України. В умовах воєнних (бойових) дій міжнародно-правові документи допускають обмеження відповідних прав і свобод.

Позиція органу правосуддя зводиться до того, що запобігання, усунення чи зменшення негативного інформаційного впливу є одним із основних способів захисту публічної безпеки. Правовий захист від негативного інформаційно-психологічного впливу набуває особливого значення в умовах злочинної війни росії проти України і Українського народу, під час широкомасштабного агресивного тиску російської федерації на суспільство та громадян через поширення недостовірної

інформації, блокування Інтернет-ресурсів, що відображають позицію України з ключових питань державної політики. У цих умовах розвивається українське законодавство, спрямоване на протидію таким проявам.

Зокрема, законодавець оперативно реагує на зовнішні та внутрішні зміни, загрози. Основним способом недопущення недостовірної інформації є встановлення відповідних критеріїв достовірності інформації, які дозволять протидіяти цьому процесу в інформаційному середовищі.

Якщо звернути увагу на окремі правові норми підзаконних актів у галузі розвитку інформаційного суспільства, то можна зробити висновок, що положення аналізованих актів торкаються не лише питань інформаційної безпеки, економічного розвитку та модернізації у сфері оборони, але й правовідносин, які виникають у процесі пошуку та створення належних умов для використання інформаційних систем і технологій.

Удосконалення правового регулювання повинно мати системний та комплексний характер, усуваючи неоднозначність понять та їх дефініцій. Фундаментальні порушення у понятійно-категоріальному апараті пов'язані з порушенням однаковості правозастосовної, зокрема судової практики через неможливість встановлення сенсу правових норм, які суперечать одна одній.

Дефекти правового регулювання позначаються на авторитеті законодавчої діяльності та ставлення громадян до закону.

Роль інформаційної безпеки та її місце у системі національної безпеки формується державною інформаційною політикою, яка взаємопов'язана з державною політикою забезпечення національної безпеки за допомогою системи інформаційної безпеки.

Державна інформаційно-правова політика є регулятором публічних і приватних правовідносин, за допомогою чого реалізуються стратегічні

завдання держави. Забезпечення інформаційної безпеки як складової національної безпеки регуляторним впливом пронизує все різноманіття суспільних відносин, що виникають у процесі життєдіяльності людини та держави.

З цього випливає, що законодавцем має проводитися вдосконалення норм публічно-правового характеру, що містять приписи та заборони, і приватноправових норм, конструкція яких полягає у дозвільному регулюванні.

Інформаційна безпека займає одне з провідних місць у системі національної безпеки, водночас існує низка проблем, які безпосередньо впливають на формування та проведення державної політики у цій сфері, включаючи такі як: різноманітність та складність інформаційного середовища; існування загрози втрати інформаційного суверенітету особи, суспільства та держави, оскільки інформаційна безпека держави перебуває на критичному рівні; не повною мірою функціонують правові механізми забезпечення конфіденційності інформації, у тому числі відомості в галузі охорони інтелектуальної діяльності.

Важливо зазначити, що правове регулювання конфіденційності інформації ґрунтується на положеннях норм Конституції України та Загальної декларації прав людини, Конвенції про захист прав людини і основоположних свобод, Міжнародного пакту про громадянські і політичні права. Особливу роль регулюванні питань інформаційної безпеки відіграють нормативно-правові акти ЄС, які мають важливе значення на етапі активних євроінтеграційних процесів в Україні, наприклад, Директива Європейського Парламенту і Ради (ЄС) 2022/2555 від 14 грудня 2022 року про заходи щодо забезпечення високого загального рівня кібербезпеки в усьому Союзі, яка вносить зміни до Регламенту (ЄС) № 910/2014 та Директиви (ЄС) 2018/1972, та скасування Директиви (ЄС) 2016/1148 (Директива NIS 2) [12].

Однак у національному законодавстві відсутня системність та несуперечність правового регулювання конфіденційної інформації. Упорядкування норм на цю тему відображено у низці правових актах, які регулюють суспільні відносини у сфері інформаційного права. У даних правових актах простежується доцільність систематизації норм, що визначають правила щодо порядку пошуку, зберігання, обробки та використання інформації конфіденційного характеру.

Складність знаходження балансу інтересів між забезпеченням безпеки та доступом до інформації за допомогою і через забезпечення конфіденційності полягає в тому, що інформація обмеженого доступу розглядається як цінність та як небезпека. Цінність державних секретів полягає у можливості їх використання для отримання користі, переваги у геополітичних протистояннях, а небезпека полягає у ризиках використання державних секретів на шкоду національній безпеці в разі порушення конфіденційності (таємності) інформації.

У випадку зі службовою таємницею проблема ускладнюється відсутністю однакового регулювання службової таємниці в різних органах державної влади. Можна констатувати відсутність ефективного правового механізму у цій сфері.

У даний час є суперечливість норм і критеріїв систематизації, які б визначали, яку інформацію можна віднести до обмеженого доступу, та відсутність упорядкованої системи регулювання конфіденційної інформації. Доцільна систематизація норм, що регулюють правовідносини порядку користування інформацією обмеженого доступу, шляхом ухвалення спеціального закону про конфіденційну інформацію, а у разі введення в дію систематизованого законодавчого акту необхідно також передбачити окремі розділи, присвячені даній проблематиці.

Водночас з'ясовано, що «правові механізми регулювання відносин у сфері забезпечення інформаційної безпеки вимагають уточнення та

доопрацювання, в частині розробки більш чітких повноважень органів, які здійснюють контрольно-наглядові заходи і перевірки органів влади, організацій та підприємств щодо дотримання вимог щодо забезпечення захисту інформації» [13, с. 53] (О. Малашко Є., С. Єсімов).

Сучасні загрози та виклики інформаційної безпеки визначили новий вектор розвитку правового регулювання безпеки в інформаційній сфері. Зокрема, законодавець посилює правовий режим обмеженого доступу до інформації. Прикладом такої політики є законодавчі зміни, внесені до Закону України «Про державну таємницю» від 27 січня 2022 року, які стосуються таємної та службової інформації, що охоплює відомості у сфері оборони [14–17].

Порядок поводження з відомостями, що становлять службову інформацію в галузі оборони, визначено в наказі Міністерства оборони України [16]. Удосконалення законодавства про інформацію обмеженого доступу було здійснено у 2022 році у питаннях кримінальної відповідальності за порушення режиму державної таємниці, правової охорони персональних даних тощо [17; 18]. Наприклад, Закон України «Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану» [18]. Це є проявом конкретних кроків щодо реалізації Стратегії інформаційної безпеки України.

Подальший розвиток міжгалузевого комплексного інституту конфіденційної інформації в інформаційному праві має низку проблем у нормативно-правовому регулюванні. Потрібні системні зміни з метою відповідності сучасним правовідносинам, що склалися між суб'єктами

права. Правова охорона конфіденційності та таємності інформації здійснюється при застосуванні спеціальних правових режимів, спрямованих на забезпечення прав, свобод і законних інтересів фізичних і юридичних осіб, громадських об'єднань та держави.

В умовах інформаційного суспільства право на доступ до інформації набуває різних аспектів і отримує подальший розвиток у діалектичному поєднанні правових режимів та різних видів інформації з обмеженим доступом.

Спеціальний правовий режим інформації часто асоціюють зі спеціальними правовими режимами. Особливий правовий режим, скоріше, відноситься до групи «надзвичайних режимів» [19], що тимчасово вводяться в умовах воєнного чи надзвичайного стану, з подальшим застосуванням тимчасових заходів економічного, військового, політичного та інших характеристик з метою запобігання негативним наслідкам для держави та національної безпеки.

Інформація конфіденційного характеру має спеціальне регульоване значення, спрямоване на забезпечення інтересів суспільства та держави. Особливі правові режими інформації застосовуються для забезпечення інформаційної безпеки в умовах надзвичайних ситуацій, воєнного або надзвичайного стану на обмежений період часу, мають спрямованість на ліквідацію або мінімізацію наслідків обставин, що склалися.

Конфіденційність реалізується шляхом взаємодії спеціальних правових режимів, спрямованих на забезпечення прав, свобод і законних інтересів людини, що ідентифікується, які створюють умови ефективного провадження діяльності в інформаційному середовищі.

В умовах цифрової трансформації набувають значення проблеми правового забезпечення безпеки при розробці та впровадженні програмних рішень та пристроїв на базі технологій штучного інтелекту, великих даних, хмарних технологій, квантових обчислень, мобільного зв'язку, Інтернету

речей та інших інформаційно-комунікаційних технологій.

Правові та технологічні ризики, які існують у цій сфері, є важко прогнозованими, вони потребують додаткових, спеціальних досліджень. В умовах впливу впровадження новітніх цифрових технологій на всі сфери інформаційного суспільства посилюється інформаційне протистояння та протиборство між демократичними та тоталітарними державами [20], розширюючи масштаби використання інформаційних систем і технологій у військово-політичних цілях, для вирішення завдань дестабілізації внутрішньодержавних відносин, підриву цифрового, технологічного, фінансового суверенітету, законності та правопорядку тощо.

У зазначених цілях створюється та поширюється інформація у спотвореному вигляді або свідомо неправдива інформація, здійснюються масовані кібератаки. У зв'язку з цим важливе значення набуває технологічний суверенітет держави, який побудований на досвіді та співпраці з державами-членами НАТО. Важливе значення має інформаційно-правова культура та цифрова грамотність громадянського суспільства.

Стан правового регулювання безпеки в інформаційній сфері в умовах російської агресії проти України показує, що основними напрямками вдосконалення законодавства у цій галузі є: забезпечення інформаційних прав і свобод, можливості реалізації не забороненим законом способом права на доступ до достовірної інформації; охорона інформації обмеженого доступу та персональних даних; протидія розповсюдженню недостовірної інформації та забезпечення інформаційно-психологічної безпеки; правове забезпечення діяльності з розробки засобів захисту інформації, технічного регулювання засобів захисту інформації, їх сертифікації та атестації згідно зі стандартами НАТО; протидія кібератакам на інформаційні ресурси, системи та об'єкти інфраструктури, у тому числі критичної інфраструктури; розвиток правового регулювання

цифрових технологій, обов'язковим компонентом якого є питання інформаційної безпеки; юридична відповідальність за протиправні дії.

Дослідження свідчить про особливе значення питання захисту та забезпечення надійного функціонування інформаційних систем і технологій, які покликані нейтралізувати внутрішні та зовнішні загрози. У зв'язку з цим законодавець реагує на кіберагресію шляхом ухвалення низки нормативно-правових актів через динамічний характер кібератак.

Висновки. Існуюча нормативно-правова база у сфері забезпечення безпеки інформаційного середовища дозволяє підвищувати ефективність захисту інформації та забезпечувати стійку роботу інформаційної інфраструктури на всіх рівнях. Дослідження показало, що в умовах цифровізації, геополітичних викликів, загроз і ризиків, соціально-економічної кризи, внаслідок злочинної війни росії проти України, загрози інформаційній безпеці посилюються, що ставить завдання удосконалення системи правового забезпечення інформаційної безпеки.

У цих умовах доцільно законодавчо закріпити правові основи забезпечення безпеки інформаційного простору з використанням інформаційно-правових засобів, які будуть спрямовані на вирішення завдань забезпечення безпеки в умовах цифровізації, геополітичних викликів і ризиків, соціально-економічної кризи, спричинених тероризмом і злочинною воєнною агресією росії проти України, на формування єдиного європейського інформаційного простору в межах Європейського Союзу та НАТО, що дозволить зміцнити організаційно-правову протидію вразливості інформаційних ресурсів, інформаційних систем і технологій та об'єктів інформаційної інфраструктури.

Література

1. Yesimov S., Borovikova V. Methodological foundations of information security research // *Social & Legal Studios*. 2023. Vol. 6, No. 1. P. 49–55.

doi: <https://doi.org/10.32518/sals1.2023.49>.

2. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 02.02.2024).
3. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 р. № 80/94-ВР (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр#Text> (дата звернення: 02.02.2024).
4. 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: 02.02.2024).
5. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text> (дата звернення: 02.02.2024).
6. Про електронні комунікації: Закон України від 16.12.2020 р. № 1089-IX (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text> (дата звернення: 02.02.2024).
7. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (дата звернення: 02.02.2024).
8. 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. № 477/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (дата звернення: 02.02.2024).

- 02.02.2024).
9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25.02.2017 р. № 47/2017 (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (дата звернення: 02.02.2024).
 10. Про національну безпеку України: Закон України від 21.06.2018 р. № 2469-VIII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (дата звернення: 02.02.2024).
 11. Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-r#Text> (дата звернення: 02.02.2024).
 12. Ковалів М. В., Петков С. В., Скриньковський Р. М., Хмиз М. В., Кокотайло Р. О., Лозинський Ю. Р., Сидор М. Я. Принципи правового забезпечення інформаційної безпеки // *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2024. № 1. doi: <https://doi.org/10.25313/2520-2308-2024-1-9566>.
 13. Малашко О. Є., Єсімов С. С. Зміст державної діяльності із забезпечення інформаційної безпеки // *Міжнародний науковий журнал «Інтернаука»*. 2020. № 15(95), т. 1. С. 46–54. doi: <https://doi.org/10.25313/2520-2057-2020-15-6341>.
 14. Про внесення змін до деяких законів України щодо уточнення завдань та основ підготовки і ведення національного спротиву: Закон України від 27.01.2022 р. № 2024-IX. URL: <https://zakon.rada.gov.ua/laws/show/2024-20#Text> (дата звернення: 02.02.2024).
 15. Про державну таємницю: Закон України від 21.01.1994 р. № 3855-XII (із змінами). URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

(дата звернення: 02.02.2024).

16. Про затвердження Переліку відомостей Міністерства оборони України, які містять службову інформацію (ПСІ-2023): Наказ Міністерства оборони України від 17.10.2023 р. № 605. URL: <https://zakon.rada.gov.ua/rada/show/v0605322-23#Text> (дата звернення: 02.02.2024).
17. *Державна таємниця як складова національної безпеки України: охорона та доступ до державної таємниці; законодавче забезпечення державної таємниці; відповідальність за розголошення державної таємниці; особливості дотримання державної таємниці під час відправлення правосуддя; особливості регулювання в особливий період та під час воєнного стану* / Укл.: Джус О. А., Золотарьова М. К., Копотун І. М., Макарова Т. П., Микитюк М. А., Павлюк О. О., Пасіка С. П., Петков С. В., Скриньковський Р. М., Сопільник Л. І., Чубенко А. Г., Шевченко А. М. Київ: ВД «Професіонал», 2023. 438 с.
18. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо забезпечення протидії несанкціонованому поширенню інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчиненому в умовах воєнного або надзвичайного стану: Закон України від 24.03.2022 р. № 2160-IX. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#Text> (дата звернення: 02.02.2024).
19. Талалай Д. В. Деякі аспекти надзвичайних правових режимів як правової форми забезпечення національної безпеки держави // *Публічне право*. 2015. № 4. С. 41–48.
20. *Україна під час російсько-української війни 2014–2023 рр.: теза*

національної стійкості крізь призму наукових досліджень: монографія / Вановська І. М., Джус О. А., Іляшко О. О., Копотун І. М., Коропатнік І. М., Первак І. О., Петков С. В., Попков Б. О., Скрябін О. Л., Стецюк С. П., Скриньковський Р. М., Сопільник Л. І., Трубчанінов М. А., Хан Є. В., Шемчук В. В.; за заг. ред. Б. Попкова, С. Петкова. Київ: Видавництво Ліра-К. 2023. 272 с.

References

1. Yesimov S., Borovikova V. Methodological foundations of information security research // *Social & Legal Studios*. 2023. Vol. 6, No. 1. P. 49–55. doi: <https://doi.org/10.32518/sals1.2023.49>.
2. Pro informatsiiu: Zakon Ukrainy vid 02.10.1992 r. № 2657-XII (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (date of access: 02.02.2024).
3. Pro zakhyst informatsii v informatsiino-komunikatsiinykh systemakh: Zakon Ukrainy vid 05.07.1994 r. № 80/94-BP (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/80/94-bp#Text> (date of access: 02.02.2024).
4. 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> (date of access: 02.02.2024).
5. Konstytutsiia Ukrainy: pryiniata na piatii sesii Verkhovnoi Rady Ukrainy 28 chervnia 1996 roku (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/254k/96-bp#Text> (date of access: 02.02.2024).
6. Pro elektronni komunikatsii: Zakon Ukrainy vid 16.12.2020 r. № 1089-IX (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>

(дата звернення: 02.02.2024).

7. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 15 zhovtnia 2021 roku «Pro Stratehiiu informatsiinoi bezpeky»: Ukaz Prezydenta Ukrainy vid 28.12.2021 r. № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text> (date of access: 02.02.2024).
8. 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. № 477/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text> (date of access: 02.02.2024).
9. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy vid 25.02.2017 r. № 47/2017 (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/47/2017#Text> (date of access: 02.02.2024).
10. Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 r. № 2469-VIII (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text> (date of access: 02.02.2024).
11. Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 r. № 1556-p (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-p#Text> (date of access: 02.02.2024).
12. Kovaliv M. V., Petkov S. V., Skrynkovskyy R. M., Khmyz M. V., Kokotailo R. O., Lozynskyy Y. R., Sydor M. Y. Pryntsypy pravovoho zabezpechennia informatsiinoi bezpeky // *Mizhnarodnyi naukovyi zhurnal «Internauka»*. Serii: «Iurydychni nauky». 2024. № 1. doi: <https://doi.org/10.25313/2520-2308-2024-1-9566>.
13. Malashko O. Y., Yesimov S. S. Zmist derzhavnoi diialnosti iz

- zabezpechennia informatsiinoi bezpeky // *Mizhnarodnyi naukovyi zhurnal «Internauka»*. 2020. № 15(95), t. 1. S. 46–54. doi: <https://doi.org/10.25313/2520-2057-2020-15-6341>.
14. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo utochnennia zavdan ta osnov pidhotovky i vedennia natsionalnoho sprotyvu: Zakon Ukrainy vid 27.01.2022 r. № 2024-IX. URL: <https://zakon.rada.gov.ua/laws/show/2024-20#Text> (date of access: 02.02.2024).
 15. Pro derzhavnu taiemnytsiu: Zakon Ukrainy vid 21.01.1994 r. № 3855-XII (iz zminamy). URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text> (date of access: 02.02.2024).
 16. Pro zatverdzhennia Pereliku vidomostei Ministerstva oborony Ukrainy, yaki mistiat sluzhbovu informatsiiu (PSI-2023): Nakaz Ministerstva oborony Ukrainy vid 17.10.2023 r. № 605. URL: <https://zakon.rada.gov.ua/rada/show/v0605322-23#Text> (date of access: 02.02.2024).
 17. Derzhavna taiemnytsia yak skladova natsionalnoi bezpeky Ukrainy: okhorona ta dostup do derzhavnoi taiemnytsi; zakonodavche zabezpechennia derzhavnoi taiemnytsi; vidpovidalnist za rozgholoshennia derzhavnoi taiemnytsi; osoblyvosti dotrymannia derzhavnoi taiemnytsi pid chas vidpravlennia pravosuddia; osoblyvosti rehuliuвання v osoblyvyi period ta pid chas voiennoho stanu / Ukl.: Dzhus O. A., Zolotarova M. K., Kopotun I. M., Makarova T. P., Mykytiuk M. A., Pavliuk O. O., Pasika S. P., Petkov S. V., Skrynkovskyy R. M., Sopilnyk L. I., Chubenko A. H., Shevchenko A. M. Kyiv: VD «Profesional», 2023. 438 s.
 18. Pro vnesennia zmin do Kryminalnoho ta Kryminalnoho protsesualnoho kodeksiv Ukrainy shchodo zabezpechennia protydii nesanktsionovanomu poshyrenniu informatsii pro napravлення, peremishchennia zbroi, ozbroiennia ta boiovykh pryipasiv v Ukrainu, rukh, peremishchennia abo

rozmishchennia Zbroinykh Syl Ukrainy chy inshykh utvorenykh vidpovidno do zakoniv Ukrainy viiskovykh formuvan, vchynenomu v umovakh voiennoho abo nadzvychainoho stanu: Zakon Ukrainy vid 24.03.2022 r. № 2160-IX. URL: <https://zakon.rada.gov.ua/laws/show/2160-20#Text> (date of access: 02.02.2024).

19. Talalai D. V. Deiaki aspekty nadzvychainykh pravovykh rezhymiv yak pravovoi formy zabezpechennia natsionalnoi bezpeky derzhavy // *Publichne pravo*. 2015. № 4. S. 41–48.
20. *Ukraina pid chas rosiisko-ukrainskoi viiny 2014–2023 rr.: geneza natsionalnoi stiikosti kriz pryzmu naukovykh doslidzhen: monohrafiia* / Vanovska I. M., Dzhus O. A., Iliashko O. O., Kopotun I. M., Koropatnik I. M., Pervak I. O., Petkov S. V., Popkov B. O., Skriabin O. L., Stetsiuk S. P., Skrynkovskyy R. M., Sopilnyk L. I., Trubchaninov M. A., Khan Y. V., Shemchuk V. V.; za zah. red. B. Popkova, S. Petkova. Kyiv: Vydavnytstvo Lira-K. 2023. 272 s.