УДК 342.59
DOI https://doi.org/10.32782/2524-0374/2023-1/71

ДІЯЛЬНІСТЬ ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ ПІД ЧАС ВІЙНИ: АДМІНІСТРАТИВНО-ПРАВОВИЙ АСПЕКТ

ACTIVITIES OF STATE AUTHORITIES TO ENSURE INFORMATION SECURITY OF UKRAINE DURING THE WAR: ADMINISTRATIVE AND LEGAL ASPECT

Литвин Н.А., д.ю.н., професор,
професор кафедри службового та медичного права
Київський національний університет імені Тараса Шевченка

Шевченко А.О., студент IV курсу
Навчально-науковий інститут економічної безпеки та митної справи
Державного податкового університету

У статті обгрунтовується важливість та значення безпеки в процесі регулювання інформаційних правовідносин з метою дотримання стабільної інформаційної безпеки в державі, зокрема в умовах війни. Проаналізовано чіткі кроки державної влади України щодо забезпечення інформаційної безпеки в окресленні адміністративно-правового аспекту. Актуальність забезпечення безпеки інформаційного простору передусім зумовлена стрімким зростанням обігу інформації серед населення, процесах її перетворення до нормативно-правової площини, яка потребує застосування попередніх перевірок разом з відповідними фахівцями щодо виявлення та прогнозування всіх наявних та можливих загроз інформаційному полю України, як в мирний час, так і в складні для держави часи повномасштабної війни. Результат та якість таких перевірок мають враховуватись під час вибору методу, способу правового регулювання інформаційних відносин. Зокрема, будуватись на засадах прозорості, відсутності обмеження конституційного права людини на інформацію.

Акцентується увага на тому, що воєнний стан не став стимулом до свавільного владного трактування та застосування суворих обмежень щодо права на інформацію та пригніченням решти конституційних прав. Поступовість та послідовність прийняття необхідних та першочергових нормативних актів, наразі є зрозумілим кроком державної влади, оскільки вони спрямовані на поновлення стабільного життя на тимчасово окупованих територіях, забезпечення безпекового положення на українських територіях та повернення такого положення на тимчасово втрачені території.

Зроблено висновки про те, що основоположним напрямом вдосконалення інформаційних правовідносин в українській державі має бути передусім безпековий підхід, так як сьогоденні реалії війни явно відображають, що інформація є не лише інструментом ведення бою, але й зброєю «масового ураження». Тому, необхідність створення єдиного впливового механізму, основним завданням якого є захист та забезпечення інформаційного поля української держави, є наразі першочерговим завданням для органів державної влади.

Ключові слова: інформація, інформаційна безпека, цифровізація, інформаційні загрози, органи державної влади, воєнний стан, захист інформаційних прав, адміністративно-правове забезпечення.

Rapid processes of informatization always entail a range of systemic changes, the presence of which entails the entry into the global information system of all spheres of activity, state institutions and almost every person. Thus, it emphasizes the need to develop a system of state steps to ensure information security, primarily guided by the principles of reliability, efficiency and the formation of a single working mechanism for strategic legal regulation of the information field. In general, the information security system in most world States has a concept as one of the most important tools for ensuring national security and government steps. Since almost daily new challenges to this security force us to adapt a stable system of countering threats, this creates a range of pressing problems that require potential scientific research in order to find ways and methods of countering, in some cases fighting. The result and quality of such methods and methods should be taken into account when implementing the procedure for legal regulation of information relations. The relevance of such approaches to building a unified system of effective support for state authorities in Ukraine is primarily due to martial law and the use of information as a "weapon of mass destruction". Thus, the subjects of rulemaking should develop a basic framework for information defense and protection of the population from "information attacks" by the aggressor country, especially in the context of accelerated European integration through the use of European information security standards. In particular, to reflect the security guarantees of the information field in the processes of its transformation and adaptation to the regulatory plane, which requires the use of preliminary checks together with relevant specialists to identify and predict all existing and possible threats to the information field of Ukraine, both in peacetime and in difficult times of full-scale war for the state. The result and quality of such checks should be taken into account when choosing the method and method of legal regulation of information relations. In particular, it should be based on the principles of transparency and the absence of restrictions on the constitutional right of a person to information.

It is emphasized that martial law has not become an incentive for arbitrary power interpretation and application of strict restrictions on the right to information and the suppression of other constitutional rights. The gradual and consistent adoption of necessary and priority normative acts is now an understandable step of the state authorities, since they are aimed at restoring stable life in the temporarily occupied territories, ensuring security in the Ukrainian territories and returning such a situation to the temporarily lost territories.

It is concluded that the fundamental direction of improving information legal relations in the Ukrainian state should be primarily a security approach, since the current realities of war clearly reflect that information is not only a tool for conducting combat, but also a weapon of "mass destruction". Therefore, the need to create a single influential mechanism, the main task of which is to protect and ensure the information field of the Ukrainian state, is now a priority task for state authorities.

Key words: information, information security, digitalization, information threats, state authorities, martial law, protection of information rights, administrative and legal support.

Постановка проблеми. Сучасний світовий прогрес та щоденна еволюція в сфері цифрових технологій, кроки до покращення інформаційного сектору, все більше набувають статусу глобальності, що проникає собою практично в усі сфери суспільного життя та буття. Варто зауважити, що процес стрімкої цифровізації зазнає перетворень як один з чинників до потенціального розвитку суспільства нового покоління, відображає собою процес соціальної динаміки. Таким чином, завдяки процесам еволюції інформаційної складової суспільного розвитку, відбувається коло змін сталої системи державного управління та адміністрування. Такі зміни здебільшого включають в себе не лише відокремлені державні інституції або певні галузі управління, але й підштовхують до змін більшість сегментів суспільства, включаючи практично кожну людину в світовий інформаційний простір. Такі зміни інформаційного простору визначають собою важливість людини як чогось глобального, таким чином підси-

люючи залежність від глобальної інформаційної мережі. У свою чергу, розгорнута Російською Федерацією повномасштабна війна на теренах української держави, підсилює наукове осмислення та актуалізує проблематику щодо забезпечення інформаційної безпеки і простору під час війни. Наразі, більшість військово-політичних конфліктів мають фазу переходу до інформаційного сектору, який постає собою в формі нового етапу зіткнення.

Аналіз останніх досліджень і публікацій. Доцільно констатувати, що безпековий аспект щодо забезпечення інформаційної безпеки, як в мирний час, так і воєнний, потребує собою постійного вдосконалення водночас привертаючи все більше уваги з боку правників. Науковому дослідженню основоположних правових стандартів та категорій, враховуючи окремі вкладення, присвячено наукові праці та доробки Арістової І., Бачила І., Веселового М., Ліпкана В., Лопатіна В., Мороза Д., Новицької Н., Олійника О., Субіної Т.В., Шапки А. та ін. При цьому враховано лише певну частину від загального наукового вкладу на заявлену тематику. Таким чином, тематика діяльності органів державної влади щодо забезпечення інформаційної безпеки не втрачає інтересу та обговорюваності серед науковців, оскільки кількість викликів сталій безпеці зростає практично щодня, особливо в період повномасштабної війни на теренах рідної країни.

Метою цієї статті є науково-теоретичне обґрунтування значення та специфічних рис безпекової політики у діяльності органів державної влади України під час війни в окресленні адміністративно-правового аспекту.

Виклад основного матеріалу. Теорія розвитку інформаційного суспільства демонструє відносно низький ступінь критичності досліджень до можливостей, які відкриваються завдяки використанню інформаційних технологій. Це призводить до недостатньої уваги до нових видів небезпек та загроз, які виникають у суспільстві внаслідок негативного впливу інформаційних технологій. Проблема інформаційної безпеки виникла на основі глобального протиріччя між можливостями інформаційних технологій, з одного боку, та негативних наслідках, небезпеки та загрози їх використання для деструктивних цілей по відношенню до особи, суспільства, держави, з іншого боку [1].

Підвищення вищевикладеної залежності сучасного інформаційного суспільства від сталого функціонування інформаційної структури, зумовлює здійснення національних інтересів української держави в інформаційному просторі та інфраструктурі обміну інформаційними даними як одного з найважливіших факторів суспільної безпеки. Таким чином, для України наразі потенційно важливим кроком на шляху до революції в галузі інформаційно-технічного майбутнього, є підвищення розроблення єдиної цілісної відносно гнучкої системи державного управління у сфері забезпечення інформаційної безпеки, яка враховуватиме перспективні тенденції, європейські стандарти щодо прогресу змін в інформаційному просторові, перебуваючи в незалежності від геополітичних навколишніх умов, економічного стану держави та здобуде відповідну підтримку українського суспільства [2, с. 39].

На сьогодні нормативно-правова та доктринальна база інформаційної безпеки в Україні розвивається симптоматично та безсистемно. Багато в чому це пов'язано з тим, що сучасні методи дослідження базуються на різних світоглядних позиціях, по-різному вирішують дослідницькі проблеми, а також використовують відмінні дослідницькі стратегії. Крім того, інформаційна безпека розглядається насамперед як інформаційна безпека держави. У подальшому активізація процесів інформатизації в усіх сферах, особливо зростання значення технічного захисту інформації, призвело до формування правового забезпечення захисту інформації як невід'ємної складової безпеки підприємств, установ і організацій та держави вцілому [1].

Аналітичне дослідження щодо застосування заходів протидії інформаційним загрозам в українській державі надає змогу побачити, що на національному рівні практично відсутня чітка державна стратегія щодо протидії таким видам загроз та забезпечення інформаційної безпеки в цілому. Більшість нормативно-правових актів виконавчої та законодавчої влади з цього напряму змістовно перетинаються між собою, проте не є систематично взаємопов'язаними, що стає причиною підсилення кібернетичних загроз та виникнення нових ризиків у системі захисту суспільства з боку державної влади. Варто сказати, що в рамках первинної протидії загрозам інформаційному сектору державна політика щодо забезпечення інформаційної безпеки здебільшого лише починає формувати базові засади та перебуває на стадії початкового розвитку. Проте, в складні часи ведення повномасштабної війни, розпочатої російською федерацією, що підтверджується Указом Президента України «Про введення воєнного стану» № 64 від 24 лютого 2022 року [3], інформаційний фронт є одним з найвпливовіших інструментів ведення війни через інформаційну пропаганду цивільного населення та розповсюдження більшості «рейкових» даних, що демонструє собою суттєву ефективність на тимчасово окупованих територіях України, розкриває слабкі місця державного інструментарію щодо протидії інформаційним загрозам.

Варто погодитись із думкою інших науковців щодо того, що сучасні вимоги інформаційної безпеки повинні ґрунтуватися на накопиченому в Європейському Союзі досвіді:

– розробки та впровадження загальнодержавних комплексних програм профілактики правопорушень та правової освіти населення;

– здійснення в рамках єдиного методологічного підходу дослідження проблем інформаційної безпеки з урахуванням кримінології та деліктології на основі аналітичної юриспруденції;

– вже існуючої соціальної політики з оптимальним поєднанням цілеспрямованих зусиль держави з ініціативи різних інститутів громадянського суспільства [1].

Впровадження європейських підходів у сфері інформаційної безпеки є необхідним кроком, так як прагнення України приєднатися до Європейського Союзу створює реальні передумови для формування системи державного управління, заходів впливу на стан і динаміку профілактичних процесів у сфері інформаційної безпеки.

Наявна проблема щодо забезпечення національних інтересів та безпеки в інформаційному середовищі наразі перебуває лише на стадії вдосконалення. Інформаційна безпека державного рівня здебільшого забезпечується в призмі національної безпеки, яка підтримується системами заходів щодо вдосконалення економічного, політичного та організаційного характерів. Таким чином, необхідним є розгляд державних методів та засобів щодо вдосконалення інформаційного поля на рівні національної безпеки, зокрема й в умовах повномасштабної війни. Першочерговим кроком до інформаційної противаги російському агресору, стало введення в дію Рішення Ради Національної Безпеки і Оборони України «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» від 18 березня 2022 року [4], що ратифіковано відповідним Указом Президента України № 152 від 19 березня 2022 року [5]. Відповідно до наявного рішення варто зазначити, що реалізація єдиної інформаційної сталої політики є одним з найприорітетніших напрямів та питань національної безпеки, забезпечення яких здійснюється шляхом об'єднання всіх загальнонаціональних телеканалів, програмно-інформаційне забезпечення яких здебільшого складається із інформаційних або інформаційно-аналітичних передач на базі єдиної інформаційної стратегічної комунікації. Варто зауважити, що запровадження такого заходу своє-

рідної суспільної безпеки на загальнонаціональному рівневі є доволі доречним кроком, оскільки інформаційні вливання з боку агресора впливають на цивільне населення найпотужнішим шляхом безпосередньо через телекомунікаційні засоби, тим самим породжуючи «фейкову» інформацію, вводячи в оману людей. Саме тому, в умовах повномасштабної війни, розв'язаною російською федерацією, фільтрування інформації є одним з першочергових заходів державного контролю та допоміжним інструментом протидії фізичній та моральній загрозам.

Культурний розвиток населення та інформаційна політика як одна з основоположних конституційних засад, що відображаються в нормах адміністративно-правового регулювання, завжди мають зовнішній вплив, проте деколи він є позитивним, деколи навпаки негативним. На превеликий жаль, правове регулювання культурного розвитку та прозорості інформаційних джерел наразі є доволі складним в рамках зазначеного стану повномасштабної війни. Проте, українська держава не полишає зусиль та продовжує боротись з процесами дестабілізації культури та мовлення українського народу. Таким чином, в рамках затвердження шостого санкційного пакету Європейського Союзу проти російської федерації [6], в Україні Міністерство культури та інформаційної політики ухвалило рішення про розширення кількості російських новинних та медіа телекомпаній, зокрема пропагандистів, які підлягають повноцінному блокуванню не лише на теренах європейських країн, але й в Україні також [7].

Продовжуючи розгляд державних кроків щодо забезпечення інформаційної безпеки під час війни в рамках адміністративно-правового аспекту, доцільно розглянути зокрема Рішення Ради Національної Безпеки і Оборони України «Про нейтралізацію загроз інформаційній безпеці держави», що введено в дію Указом Президента України № 151 від 18 березня, 2022 року [8]. Даним нормативним актом регламентовано об'єднання зусиль Державної служби спеціального зв'язку та захисту інформації України з приватними компаніями щодо контролю радіомовлення, радіозв'язку та телебачення на період воєнного стану. Зокрема, це стосується здійснення цілодобового моніторингу ефірних мереж, супутникових та наземних каналів зв'язку з метою виявлення ворожої інформації або несанкціонованого втручання. Ми вважаємо, що такі ретельні заходи становлять собою доволі вагому важливість в аспекті забезпечення безпеки інформації, оскільки радіомовлення, радіозв'язок наразі є динамічним та практично нефільтрованим інструментарієм ведення суспільного інформування, що потребує собою втручання з боку органів державної влади вже декілька років. Таким чином, постійний моніторинг обміну інформаційними даними між телекомунікаційними підприємствами приватного рівня надасть змогу унеможливити не лише публікування забороненої інформації, але й контролювати та протидіяти «інформаційним вкидам» та сприянню ефективності інформаційного поля на приватному рівні.

Доцільно зазначити, що в рамках адміністративно-правового регулювання інформаційного поля країни, застосовуються не лише технічні заходи первинного рівня, але й звернення до національних джерел адміністративного права. Таким чином, Стратегія інформаційної безпеки, прийнята в 2021 році наразі залишається актуальною, оскільки передбачає собою комплексну структурну взаємодію на основі Конституції України, законів та інших нормативних актів [9]. Варто відмітити, що аналіз більшості очікуваних та наявних результатів Стратегії дає підстави вважати, що вона здебільшого спрямована на: захист інформаційного простору, підвищення ефективності щодо функціонування системи стратегічних комунікацій, реалізацію ефективної протидії щодо поширення протизаконного контенту, сприяння сталому процесові інформаційної інтеграції громадського населення, що перебуває або проживає на тимчасовоокупованих територіях до глобальної української системи обміну інформацією, сприяння захисту прав журналістів та формування єдиної української громадянської ідентичності, якої позбавити український народ й досі не полишають спроби російські загарбники.

Не стає виключенням й те, що в умовах повномасштабної війни змінюється практично все. Також, підпадають до змін й акценти уваги щодо якості виявлення загроз, реакція на їх виявлення, більшість процесів протидії будь-яким формам окупаційної загрози першочергово реалізується в напрямі людиноцентризму та поступовому звуженню прав людини, спираючись на необхідність протидії впливу реально існуючих загроз. Зокрема, варто вказати, що воєнний стан не став стимулом до свавільного владного трактування та застосування суворих обмежень щодо права на інформацію та пригніченням решти конституційних прав. Поступовість та послідовність прийняття необхідних та першочергових нормативних актів, наразі є зрозумілим кроком державної влади, оскільки вони спрямовані на поновлення стабільного життя на тимчасово окупованих територіях, забезпечення безпекового положення на українських територіях та повернення такого положення на тимчасово втрачені території.

Отже, з моменту проголошення воєнного стану, всі зміни приймаються відповідно до новітніх реалій та викликів війни. Загалом вони спрямовані на врегулювання деяких аспектів інформаційних правовідносин та інформаційного обігу серед населення, врегулювання правовідносин щодо заборони та поширення стратегічно важливої інформації, правового регулювання в аспекті технічного фіксування подій які становлять собою важливість державного рівня, встановлення або посилення юридичної відповідальності за поширення забороненої інформації та врегулювання процесуального аспекту щодо своєчасної протидії таким діям і вилученню інформаційних даних.

Висновки та перспективи подальших розвідок. На підставі вищевикладеного варто наголосити, що основоположним напрямом вдосконалення інформаційних правовідносин в українській державі має бути передусім безпековий підхід. Сьогоденні реалії війни явно відображають, що інформація є не лише інструментом ведення бою, але й зброєю «масового ураження». Таким чином, необхідність створення єдиного впливового механізму, основним завданням якого є захист та забезпечення інформаційного поля української держави, водночас з дотриманням конституційних прав людини, є наразі першочерговим завданням для органів державної влади. Найбільша соціальна цінність українського народу полягає у розумінні та особистому сприйнятті для кожного понять «справедливість» та «свобода». Нажаль, їх дотримання та незалежність дається дуже тяжко і коштує власного життя. Саме тому, формування єдиної дієвої державної політики щодо забезпечення інформаційної безпеки в умовах війни є наразі актуальною, комплексною технічною та організаційно-політичною діяльністю, яка спрямована на захист держави, суспільства і людини відповідно до сучасних європейських ідеологій. Воєнний та мирний час мають суттєві розбіжності, які полягають в тому, що перспектива захисту інформаційного сектору в воєнний час є пріоритетом, оскільки від неї залежить доля людських життів та безпека решти суспільства, водночас як в мирний, інформація слугує лише інструментарієм для обміну даними, отримання зовнішнього вияву у приватноправових відносинах.

Інформаційне поле та безпека наразі є одним з потенційно обговорюваних факторів на вустах не лише населення, але й державних службовців. Щоденні зміни до загальних правил поведінки в нормативно-правових актах

породжують собою не лише ефективність, але й виникнення вагомого кола колізійних питань та проявів, які потребують собою постійного моніторингу та пошуку шляхів вдосконалення або зміни. Таким чином, перспектива подальших розвідок даної теми, має передове місце не лише у воєнний час, але й в післявоєнний та мирні часи загалом.

ЛІТЕРАТУРА

1. Fedorenko, V.; Lytvyn, N.; Luchenko, D.; Panova, I.; Tsybulnyk, N. Legal aspects of information security management in the conditions of Ukraine's European integration. *Journal of Security and Sustainability Issues* 10(2): 2020 Volume 10 Number 2 December. P. 477–489. URL: https://jssidoi.org/jssi/papers/papers/journal/41

2. Ткачук Т.Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. *Вісник* Ужгородського національного університету. Ужгород. 2017. № 2 (46). С. 39–42.

3. Про введення воєнного стану в Україні: Указ Президента України № 64 від 24.02.2022 року. Офіційний портал Президента України. URL: https://www.president.gov.ua/documents/642022-41397

4. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану: Рішення Ради національної безпеки і оборони України № n_0004525-22 від 18.03.2022 року. *Відомості Верховної Ради України*. URL: https://zakon.rada.gov.ua/laws/show/n0004525-22#n2

5. Про Рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану» : Указ Президента України № 152 від 19.03.2022 року. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/152/2022#Text

6. Russian war with Ukraine: Europe adopts sixth package against Russia. Official page of the European Union. URL: https://ec.europa.eu/commission/presscorner/detail/ru/IP_22_2802

7. МКІП наполягатиме на розширенні кількості російських телекомпаній, що підпадають під санкції ЄС. Офіційний портал мультимедійної платформи іномовлення України Укрінформ. URL: https://cutt.ly/HMpYffP

8. Про рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Про нейтралізацію загроз інформаційній безпеці держави» : Указ Президента України № 151 від 19.03.2022 року. Офіційний портал Ради безпеки і оборони України. URL: https://www.rnbo.gov.ua/ua/Ukazy/5294.html

9. Стратегія інформаційної безпеки України: Указ Президента України № 685 від 28.12.2021 року. *Відомості Верховної Ради України.* URL: https://zakon.rada.gov.ua/laws/show/685/2021#n14