

Світлана Мазепа,

доцент кафедри кримінального права та процесу
Західноукраїнського національного університету,
міжнародний дослідник
Оснабрюцького університету
ORCID: <https://orcid.org/0000-0003-1282-9089>

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ: ПЕРСПЕКТИВИ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Сьогодні підвищується важливість інформації у житті суспільства та зростає кількість людей, зайнятих у сфері інформаційної індустрії. Настає не просто черговий етап науково-технічного прогресу, а нова ера у розвитку людства, оскільки йдеться про становлення інформаційного суспільства в умовах глобалізації. Багато країн світу співвідносять свої державні інтереси з розвитком інформаційної інфраструктури, активністю інформаційної взаємодії з громадянським суспільством та засобами масової інформації.

Аналіз сучасної правової наукової літератури свідчить про відсутність єдиного підходу до понять «інформація» та «інформаційна безпека», демонструється «вузький» та «широкий» підходи до їхнього сприйняття.

У статті розглядається розвиток поняття «інформаційна безпека» в нормативно-правових актах, взаємозв'язок її сутнісного змісту з базовими законодавчими актами у сфері безпеки, а також узагальнюються наявні знання щодо визначення місця інформаційної безпеки в системі національної безпеки України.

Ключові слова: національна безпека, інформаційна безпека, безпека інформації, загроза інформаційній безпеці, Стратегія інформаційної безпеки.

Мазепа С.

Ensuring information security in Ukraine: prospects for administrative and legal regulation

Currently, the importance of information in the life of society is increasing and the number of people employed in the information industry is growing. It is not just another stage of scientific and technological progress, but a new era in the development of mankind, as it is about the formation of the information society in the context of globalization. Many countries have begun to correlate their national interests with the development of information infrastructure and active information interaction with civil society and the media.

The analysis of the modern legal scientific literature shows that there is no single approach to the concepts of «information» and «information security», and the author demonstrates «narrow» and «broad» approaches to their perception.

The article discusses the development of the concept of «information security» in legal acts, the relationship of its essential content with the basic legislative acts in the field of security, and also summarizes the available knowledge on determining the place of information security in the national security system of Ukraine.

Keywords: national security, information security, information security, threat to information security, information security strategy.

Постановка проблеми. У сучасних військово-політичних реаліях важко і навіть недоречно запевнати роль інформації як інструменту протистояння країні-агресору. Інформація дає змогу перемагати у війнах і політичних кризах без жодного пострілу, породжуючи та посилюючи внутрішні конфлікти. Така тактика характерна для нової форми ведення війни – гібридної, у якій безпосередній інформаційний елемент є лише одним із компонентів військових дій. Свідомість осіб, які сприймають інформацію, знає постійного інформаційного впливу. Щоб відфільтрувати позитивний і негативний вплив, людині необхідно мати усвідомлену систему власних цінностей і пріоритетів, а також навички безпечної роботи в Інтернеті. Становлення інформаційної культури призвело до зниження здатності людини до критичного сприйняття, важливого значення набули аналіз і оцінювання отриманої інформації. У такому разі здатність до формування власної думки практично відсутня.

Аналіз останніх досліджень і публікацій. Адміністративно-правові аспекти забезпечення інформаційних прав, свобод і законних інтересів в інформаційному просторі, в т. ч. інформаційної безпеки,

досліджувалися в працях: В. Б. Авер'янова, В. М. Бевзенка, А. І. Берлача, Ю. П. Битяк, Н. П., І. С. Гриценко, Л. С. Кисіль, В. К. Колпакова, О. В. Кузьменко, Р. С. Мельник, А. О. Селіванова, Ю. С. Шемчушенко та ін.

З точки зору адміністративного права, окремо розглянуто відповідні питання, передбачені законами про інформаційну безпеку, але більшість з них орієнтована на національну безпеку, охоплюючи національну безпеку в інформаційній сфері та модель розвитку інформаційного суспільства. Ці та інші споріднені питання досліджувалися в наукових роботах іноземних науковців: Named Taherdoost, Farid, Ghulam, Fatima, Nosheen, Iftikhar, Sadaf, Mijwil, Maad, Aljanabi, Mohammad, Ali, Ahmed, van Niekerk, Johan.

Сьогодні вказана тема заслуговує пильної уваги на питання забезпечення інформаційної безпеки як особистості, так і суспільства загалом та необхідності комплексного дослідження в умовах цифрової трансформації.

Мета дослідження – комплексний аналіз адміністративно-правових основ інформаційної безпеки в Україні та розроблення рекомендацій щодо його вдосконалення.

Виклад основного матеріалу дослідження. В Україні простежується зростання ролі інформаційної сфери, переосмислення її значення як найважливішого фактора життя, що безпосередньо впливає на всі види національної безпеки, у зв'язку з чим у країні динамічно розвиваються процеси інформатизації. Тому особливого значення набувають такі поняття, як: «електронне урядування», «електронний уряд», «електронна держава» і т. д.

Все частіше виникає потреба правового оцінювання та регламентації інформаційних відносин. Склалося розуміння, що якими б складними не були наслідки інформаційної війни, що почалася проти України, свобода інформації – це неодмінний атрибут громадянського суспільства, що будується. Захист інформаційного простору в цих умовах є одним із базових завдань і суспільства, і держави. Відповідно, інформаційна безпека набуває все більшої значущості в загальній системі національної безпеки країни загалом. Усі дослідники вказаної проблеми ставили питання місце інформаційної безпеки у системі безпеки взагалі. Арістова В. І., Сулацький Д. В., наприклад, підкреслюють, що інформаційна безпека країни – це окремий напрямок, який нині для деяких держав має навіть більший пріоритет, ніж ядерна безпека [1, с. 115].

На думку Ментух Н. Ф. (*N. Mentukh, O. Shevchuk, M. Verbitska, T. Kuz, (2023)*), національна безпека України суттєво залежить від інформаційної безпеки, і в ході технічного прогресу ця залежність зростатиме [2, с. 76].

Братасюк О. (*O. Bratasyuk, O. Shevchuk (2023)*) зазначає, що в сучасних умовах захищеність інформації висувається на перший план, стає одним із основних елементів національної безпеки та є пріоритетним напрямом розвитку будь-якої держави [3, с. 23].

Войтко О. В., відштовхуючись від аналізу стратегічних документів, констатує, що інформаційна сфера є системотворчим фактором життя суспільства, вона активно впливає на стан політичної, економічної, оборонної та інших складових безпеки України, а забезпечення інформаційної безпеки відіграє ключову роль у забезпеченні національної безпеки країни [4, с. 165].

У нормативно-правовій основі України це питання також залишено поза увагою. У Стратегії інформаційної безпеки України визначено, що інформаційна безпека держави є однією зі складових національної безпеки. Передбачено, що система організації інформаційної безпеки є частиною системи національної безпеки. Зокрема, у Стратегії зазначено: «...інформаційна безпека України – складова частина національної безпеки України, 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 ефективна 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...» [5].

Неодноразово зазначалося, що нормативна база, пов'язана з проблемами національної безпеки, охоплює чимало різноманітних розрізнених актів, у яких понятійний апарат суперечливий і далекий від досконалості. Це повною мірою також стосується видових категорій національної безпеки, у т. ч. інформаційної.

Подібне становище багато в чому пояснюється тим, що поняття «інформаційна безпека» ще не має достатньої теоретичної бази, воно є вкрай складним для тлумачення, а різноманіття підходів до його

інтерпретації лише ускладнює ситуацію. Деякі науковці стверджують, що поняття «інформаційна безпека» з'явилося у вітчизняній науці у 1990-х роках. XX ст. щодо захисту комп'ютерної інформації (баз даних, комп'ютерних мереж). Було створено робочу комісію з удосконалення системи національної безпеки. [6]

Вважаємо, що для більш чіткого визначення предметної галузі законодавства у сфері інформаційної безпеки пропонувалося виокремити три підгрупи об'єктів захисту. До них належать:

– захист інформації та прав на неї (у т. ч. право на доступ до інформації, право на таємницю, права на об'єкти інтелектуальної власності);

– захист людини та суспільства від впливу «шкідливої» інформації; захист інформаційних систем та прав на них (у т. ч. прав та інтересів держави щодо збереження єдиного інформаційного простору в країні).

Загалом окремі загрози національній безпеці України в інформаційній сфері становлять сукупність умов і факторів, що створюють загрозу життєво важливим інтересам держави, суспільства та особи внаслідок можливого негативного впливу інформації на свідомість та особистість, поведінка громадян, інформаційні ресурси та інфраструктура інформаційних технологій [7, с. 2].

Сьогодні дослідження проблеми інформаційної безпеки привертає величезну увагу представників різних наук. Багато вітчизняних науковців безпосередньо вивчали теоретичні основи категоріального апарату інформаційної безпеки [6; 12].

Інформаційна безпека – складне системне, багаторівневе явище, на стан та перспективи розвитку якого прямо впливають зовнішні та внутрішні чинники. Термін «інформаційна безпека» розуміється у «вузькому» та «широкому» значенні. У «вузькому» сенсі інформаційна безпека сприймається як набір апаратних і програмних засобів гарантування безпеки, доступності й конфіденційності даних у комп'ютерних мережах.

Мотивація авторів цього підходу проста: те, що у 1970-ті роки називалося комп'ютерною безпекою, а 1980-ті роки – безпекою даних, сьогодні називається інформаційною безпекою. Згідно з подібною логікою, Дж. Ван Нікерк (*Johan van Niekerk. (2013)*) стверджує, що «інформаційна безпека» – це заходи щодо захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття та затримок у доступі [8].

Тут використовувався термін «критичні дані», тобто дані, що вимагають захисту через ймовірність (ризик) завдання різної шкоди в тому випадку, якщо відбудеться їх випадкове або навмисне розкриття, зміна або руйнування. Відповідно, мета інформаційної безпеки полягає в тому, щоб убезпечити цінності системи, захистити та гарантувати точність та цілісність інформації та мінімізувати руйнування, які можуть відбутись. Інформаційна безпека гарантує досягнення таких цілей:

- конфіденційність критичної інформації;
- цілісність інформації та пов'язаних з нею процесів (створення, введення, обробка та виведення);
- доступність інформації, коли вона потрібна;
- облік всіх процесів, пов'язаних з інформацією.

У «широкому» сенсі інформаційну безпеку вивчали дослідники, які відштовхувалися від положень Стратегії інформаційної безпеки України, де під інформаційною безпекою розуміється: «... 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...» [5].

На основі національних інтересів України в інформаційній сфері формуються стратегічні та поточні завдання внутрішньої та зовнішньої політики держави щодо гарантування інформаційної безпеки, тобто тут інформаційна безпека – це стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використання та розвиток на користь громадян, організацій та держави.

Таким чином, під інформаційною безпекою, на думку М. Маад (*Mijwil, Maad & Aljanabi, Mohammad & Ali, Ahmed. (2023)*), визначено захищеність інформації та підтримуючої інфраструктури від випадкових чи навмисних впливів природного чи штучного характеру, які можуть завдати неприйнятної шкоди суб'єктам інформаційних відносин, у т. ч. власникам та користувачам інформації та підтримуючої інфраструктури [9].

Свій варіант визначення пропонували Ф. Гулам (*Farid, Ghulam & Fatima, Nosheen & Iftikhar, Sadaf (2023)*), для них інформаційна безпека – стан захищеності життєво важливих інтересів особистості, суспільства та держави в інформаційній сфері від зовнішніх та внутрішніх загроз, що забезпечує її формування, використання та розвиток [10].

Вважаємо, що у визначенні розробників Стратегії інформаційної безпеки України родовою, тобто загальною ознакою «інформаційної безпеки», є «стан захищеності національних інтересів в інформаційній сфері». Видова ознака поняття «інформаційна безпека» полягає у вказівці на те, що національні інтереси визначаються «сукупністю збалансованих інтересів особи, суспільства та держави» [5].

Тахердуст Х. (Hamed Taherdoost (2022)) зазначав, що формально інформаційна безпека – це стан захищеності основних сфер життєдіяльності щодо небезпечних інформаційних впливів. Він наголошував, що найнебезпечніші інформаційні впливи називають інформаційною зброєю, до якої належать засоби знищення або розкрадання інформаційних масивів, добування з них необхідної інформації після подолання системи захисту, обмеження або заборони доступу до них законних користувачів, а також дезорганізація роботи технічних засобів, висновок з ладу телекомунікаційних мереж, комп'ютерних систем, усіх засобів високотехнологічного забезпечення життя суспільства та функціонування держави [11].

Інформаційна безпека передбачає не лише захист від інформаційної зброї, а й забезпечення конституційних прав громадян на свободу збору, розповсюдження та отримання інформації (природно, з певними обмеженнями), на таємницю кореспонденції тощо. Таким чином, інформаційна безпека передбачає певний баланс інтересів особистості, суспільства та держави. Такий баланс можливий лише у випадку, коли конкретний індивід та суспільство загалом захищені від небезпечного інформаційного впливу з боку держави. Водночас держава має право захищати своїх громадян від шкідливого інформаційного впливу ззовні.

Цікавий підхід надають Богданович В. Ю., Павловський О. В., які вважають, що логічно було б сформулювати визначення інформаційної безпеки не через категорію «національні інтереси», а через категорію «безпека інформації», уточнюючи, що не вся інформаційна сфера є об'єктом інформаційної безпеки рамках забезпечення державної безпеки [13, с. 10].

Інформаційна безпека розглядається тут не лише як самостійний напрямок, а й як ключова складова забезпечення комплексної безпеки інших сфер життєдіяльності особистості, суспільства та держави. Потрібно звернути увагу, що основна формула всіх визначень (і нормативних, і наукових) – це «захищеність», оскільки саме подібний підхід виражає традицію вітчизняної наукової думки в розумінні категорії «безпека».

Вкрай своєрідний підхід демонструє Л. Часалов (*Mishra, Sushma & Chasalow, Lewis. (2011)*). Не маючи можливості докладно зупинитися на його оригінальних ідеях, сформулюємо базові моменти.

1. Безпека – це не стан захищеності, безпеку слід розуміти як ситуацію, за якої об'єкту безпеки не може бути завдано шкоди у вигляді деструкції, дисфункції, погіршення умов існування.

2. Інформаційна безпека – це насамперед безпека від інформації, а не безпека інформації. Специфіка інформаційної безпеки полягає в тому, що йдеться про можливість заподіяння шкоди за допомогою інформаційного дії або через вплив на інформаційну інфраструктуру об'єкта безпеки, яким є соціальний суб'єкт.

3. Головні об'єкти інформаційної безпеки – людина та її свідомість, а не комп'ютер та його програми [14].

Отже, як саме поняття «інформаційна безпека», так і зміст забезпечення інформаційної безпеки потребує чіткого розуміння того, як законодавець представляє національні інтереси та загрози у сфері інформаційної безпеки України. Пропозиції щодо удосконалення відповідальності за порушення у цій сфері досліджувалися у попередніх працях [15].

Висновки. Лише за умов взаємодії людей і держави можна реально й ефективно забезпечити інформаційну безпеку. Адже якщо людина не дбає про власну інформаційну безпеку, то політика будь-якої країни щодо забезпечення інформаційної безпеки не принесе позитивних результатів. І навпаки, як би людина не намагалася протидіяти негативному інформаційному впливу, вона сама без допомоги держави не зможе впоратися з щоденним потоком інформації, яка постійно дискредитує державу та все, що з нею пов'язане. Держава створює умови для інформаційної безпеки в Інтернет-просторі, а особи несуть відповідальність за отриману інформацію та дії, вчинені під її впливом.

Отже, гарантування інформаційної безпеки є діяльністю уповноважених органів і посадових осіб, яка здійснюється в межах, встановлених законодавством, і спрямована на дотримання прав і свобод особи під час взаємодії з інформацією, отриманою з Інтернет-простору (на основі сприйняття, обробки та подальшої дії інформації, захист персональних даних користувачів Інтернету), а також гарантування національної безпеки від деструктивного впливу інших країн або певних сил в Інтернет-просторі.

Список використаних джерел

1. Арістова В. І., Сулацький Д. В. Інформаційна безпека людини як споживача телекомунікаційних послуг : монографія. Київ : Право України, 2013. 184 с.
2. Nataliya Felikissimivna Mentukh, Oksana Romanivna Shevchuk, Verbitska Mariana Vasylivna, Kuz Tetiana Volodymyrivna. *Ensuring Information Security: Comparative Legal Aspect. Central European Management Journal*. 2023. No 31 (3). P. 74–87. Retrieved from https://journals.kozminski.cem-j.org/index.php/pl_cemj/article/view/917 (date of application: 10.02.2024)
3. Oksana Bratasyuk, Oksana Shevchuk Protection of children’s information (digital) rights who were illegally exported from the territory of Ukraine during the war or in occupation. *Visegrad Journal on Human Rights*. 2022. No 2. P. 21–26. https://journal-vjhr.sk/wp-content/uploads/2022/06/VJHR_2_2022_Last.pdf (date of application: 11.02.2024)
4. Войтко О. В. Реалізація державної інформаційної політики та забезпечення інформаційної безпеки в умовах конфлікту з Російською Федерацією. *Грааль науки*. 2021. № 1. С. 164–166. URL: <https://doi.org/10.36074/grail-of-science.19.02.2021.030> (дата звернення: 07.02.2024)
5. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки» : Указ Президента України 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n7> (дата звернення: 10.02.2024)
6. Чистоклегов Л. Г., Хитра О. Л. Адміністративно-правові засоби у забезпеченні інформаційної безпеки України. ІТ-право: проблеми та перспективи розвитку в Україні : зб. матеріалів II-ї Міжнар. наук.-практ. конф. (Львів, 17 листоп. 2017 р.). Львів, 2017. С. 212–217. URL: <http://aphd.ua/publication-349/> (дата звернення: 12.02.2024)
7. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. URL: <http://www.justinian.com.ua/article.php?id=3222> (дата звернення: 10.02.2024)
8. van Niekerk, Johan. From information security to cyber security. *Computers & Security*. 2013. No 38. 97–102. 10.1016/j.cose.2013.04.004.
9. Mijwil, Maad & Aljanabi, Mohammad & Ali, Ahmed. (2023). ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information. 2023. 10.58496/MJCS/2023/004.
10. Farid, Ghulam & Fatima, Nosheen & Iftikhar, Sadaf. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*. 1–15. 10.1177/01655515231160026.
11. Hamed Taherdoost, Cybersecurity vs. Information Security. *Procedia Computer Science*. 2022. Volume 215. P. 483–487. URL: <https://doi.org/10.1016/j.procs.2022.12.050> (date of application: 10.02.2024)
12. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. Актуальні проблеми вітчизняної юриспруденції. 2022. № 1. С. 152.
13. Богданович В. Ю., Павловський О. В. Комплексна модель управління інтегрованим потенціалом протидії загрозам воєнного характеру для забезпечення визначеного рівня воєнної безпеки держави. Розвиток та застосування Повітряних сил, інших видів Збройних сил України, удосконалення їх системи управління. 2017. С. 6–11.
14. Mishra, Sushma & Chasalow, Lewis (2011). Information Security Effectiveness: A Research Framework. *Issues in Information Systems*. 12. 246–255.
15. Mazepa S., Bratasyuk O. Die Gewährleistung der Informationssicherheit in der Ukraine–Verwaltungs-und strafrechtliche Maßnahmen. *OER Osteuropa Recht*. 2023. T. 68. №. 4. С. 421–442.

References

1. Aristova, V. I. & Sulatskyi, D. V. (2013). *Informatsiyna bezpeka lyudyny yak spozhyvacha telekomunikatsiynykh posluh: monohrafiia [Information security of a person as a consumer of telecommunication services: monograph]*. Kyiv [in Ukrainian]
2. Mentukh, Nataliya Felikissimivna, Shevchuk Oksana Romanivna, Verbitska, Mariana Yuriiivna & Kuz, Tetiana Volodymyrivna (2023). Ensuring Information Security: Comparative Legal Aspect. *Central European Management Journal*, 31(3), 74–87. Retrieved from https://journals.kozminski.cem-j.org/index.php/pl_cemj/article/view/917 [in English]
3. Bratasyuk, Oksana & Shevchuk Oksana [2022]. Protection of children’s information (digital) rights who were illegally exported from the territory of Ukraine during the war or in occupation. *Visegrad Journal on*

- Human Rights*, 2, 21- 26. Retrieved from https://journal-vjhr.sk/wp-content/uploads/2022/06/VJHR_2_2022_Last.pdf [In English]
4. Voitko, O. V. (2021). *Realizatsiya derzhavnoyi informatsiynoyi polityky ta zabezpechennya informatsiynoyi bezpeky v umovakh konfliktu z Rosiyskoyu Federatsiyeyu. Mizhnarodnyy zhurnal «Hraal nauky» [Implementation of the state information policy and ensuring information security in the conditions of the conflict with the Russian Federation. International journal «Grail of Science», 1, 164–166.* Retrieved from <https://doi.org/10.36074/grail-of-science.19.02.2021.030> [in Ukrainian]
 5. *Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrainy vid 15 zhovtnya 2021 roku «Pro Stratehiyu informatsiynoyi bezpeky» [On the decision of the National Security and Defense Council of Ukraine dated October 15, 2021 «On Information Security Strategy»: Decree of the President of Ukraine of December 28, 2021 No. 685/2021].* Retrieved from <https://zakon.rada.gov.ua/laws/show/685/2021#n7> (Date of application 03/20/2024) [in Ukrainian]
 6. Chistokletov, L. G. & Khytra, O. L. (2017). *Administratyvno-pravovi zasoby u zabezpechenni informatsiynoyi bezpeky Ukraini [Administrative and legal means of ensuring information security in Ukraine]. IT-pravo: problemy ta perspektivy rozvytku v Ukraini: Zb. materialiv II-yi Mizhnar. nauk.-prakt. konf. - Administrative and legal means in ensuring information security in Ukraine: Collection. materials of the II International science and practice conf. (Lviv, November 17, 2017).* Lviv, 212–217. Retrieved from <http://aphd.ua/publication-349> [in Ukrainian]
 7. Petryk, V. *Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [The essence of information security of the state, society and the individual]. Rezhym dostupu.* Retrieved from <http://www.justinian.com.ua/article.php?id=3222> [in English]
 8. van Niekerk, Johan. (2013). From information security to cyber security. *Computers & Security*. 38. 97-102. 10.1016/j.cose.2013.04.004 [in English]
 9. Mijwil, Maad & Aljanabi, Mohammad & Ali, Ahmed (2023). *ChatGPT: Exploring the Role of Cybersecurity in the Protection of Medical Information.* 2023. 10.58496/MJCS/2023/004 [in English]
 10. Farid, Ghulam & Fatima, Nosheen & Iftikhar, Sadaf. (2023). Digital information security management policy in academic libraries: A systematic review (2010–2022). *Journal of Information Science*, 1-15. 10.1177/01655515231160026 [in English]
 11. Hamed, Taherdoost (2022). Cybersecurity vs. Information Security. *Procedia Computer Science*, 215, 483-487. Retrieved from <https://doi.org/10.1016/j.procs.2022.12.050> [in English]
 12. Koterlin, I. B. (2022). *Informatsiyna bezpeka v umovakh voyennoho stanu u aspekti zabezpechennya informatsiynykh prav ta svobod [Information security under martial law in the aspect of ensuring informational rights and freedoms]. Aktualni problemy vitchyznyanoyi yurysprudentsiyi – Actual problems of domestic jurisprudence, 1, 152* [in Ukrainian]
 13. Bohdanovich, V. Yu. & Pavlovskiy O. V. (2017). *Kompleksna model upravlinnya intehrovanyim potentsialom protydyi zahrozam voyennoho kharakteru dlya zabezpechennya vyznachenoho rivnya voyennoi bezpeky derzhavy [A comprehensive model of managing the integrated potential of countering threats of a military nature to ensure a certain level of military security of the state]. Development and application of the Air Force, other types of Armed Forces of Ukraine, improvement of their management system, 6–11* [in Ukrainian]
 14. Mishra, Sushma & Chasalow, Lewis. (2011). Information Security Effectiveness: A Research Framework, Issues in Information Systems. *Issues in Information Systems*, 12, 246-255 [in English]
 15. Mazepa, S. & Bratasyuk, O. (2023). Die Gewährleistung der Informationssicherheit in der Ukraine-Verwaltungs-und strafrechtliche Maßnahmen. *OER Osteuropa Recht*, 68 (4), 421-442 [in German]

Стаття надійшла до редакції 18.02.2024 р.