УДК 340:355/004
DOI 10.31732/2708-339X-2024-11-A15

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ДЕТЕРМІНАНТА ЗБЕРЕЖЕННЯ УКРАЇНСЬКОЇ ДЕРЖАВНОСТІ В УМОВАХ ВЕДЕННЯ ВІЙНИ

Биков О.М.,
доктор юридичних наук, професор,
професор кафедри теорії та історії держави і права
Університет економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: oleksandrbm@krok.edu.ua
ORCID: https://orcid.org/0000-0003-4965-696X

INFORMATION SECURITY AS A DETERMINANT OF PRESERVING UKRAINIAN STATEHOOD IN TIMES OF WAR

Bykov O.M.,
Doctor of Laws, Professor,
Professor of the Department of State and
Legal Disciplines of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: oleksandrbm@krok.edu.ua
ORCID: https://orcid.org/0000-0003-4965-696X

Анотація. *Проблема забезпечення інформаційної безпеки в глобальному світі не оминула й Україну. Наша держава, особливо з початком повномасштабної російсько-української війни, постійно потерпає від кібератак на інформаційну інфраструктуру держави (програмне забезпечення органів державної влади, державні сайти, інформаційно-технічне забезпечення стратегічних державних об'єктів, банківських установ), тотального антиукраїнського інформаційного впливу, поширення дезінформації, просування ідей сепаратизму, розбрату та насильства. Ворог, за допомогою найрізноманітніших технік інформаційного впливу на українців, намагається підірвати основи національної безпеки держави, посягнути на культурну ідентичність українського народу, зруйнувати дипломатичні стосунки та міжнародні домовленості між Україною та її стратегічними партнерами, розпалити всередині країни міжнаціональні, міжконфесійні конфлікти, і врешті, посягнути на конституційний лад та територіальну цілісність держави.*

Не тільки вітчизняні медіаресурси сьогодні, але навіть відомі світові видання, в силу різних обставин, часто висвітлюють інформацію та події, які відбуваються в Україні однобічно чи неповно, порушуючи її цілісність. Населення держави в умовах гібридної війни дедалі більше зазнає інформаційно-психологічного тиску на свідомість. Усе наведене свідчить про необхідність вироблення в Україні механізмів потужного захисту конфіденційності, доступності та цілісності інформації, що унеможливить різного роду посягання на законні права та інтереси громадян, приватних та державних організацій, держави в цілому.

У статті висвітлено зв'язок інформаційної безпеки з її родовою категорією – національною безпекою, проаналізовано чинники, які впливають на цілісність, доступність та конфіденційність інформації. Звернено увагу читача на необхідності розвитку інформаційної культури суспільства, що дозволить чинити гідний опір тим загрозам, які постають перед сучасною Україною в умовах повномасштабної, і водночас, гібридної війни з потужною інформаційною складовою.

Ключові слова: *інформація, інформаційна безпека, інформаційний простір, національна безпека, інформаційна культура, медійна та інформаційна грамотність, гібридна війна,*

інформаційне право.

***Формул**: 0; рис.: 0, табл.: 0, бібл.: 11.*

***Abstract**. The issue of ensuring information security in the global world has not bypassed Ukraine. Especially since the onset of the full-scale Russian-Ukrainian war, our country constantly suffers from cyberattacks on the state's information infrastructure (government software, state websites, information and technical support of strategic state objects, banking institutions), total anti-Ukrainian informational influence, dissemination of disinformation, promotion of separatist ideas, discord, and violence. The enemy, using various techniques of informational influence on Ukrainians, seeks to undermine the foundations of the state's national security, encroach on the cultural identity of the Ukrainian people, destroy diplomatic relations and international agreements between Ukraine and its strategic partners, ignite intra-country interethnic, interconfessional conflicts, and ultimately, encroach on the constitutional order and territorial integrity of the state. Not only domestic media resources today, but even well-known world publications, due to various circumstances, often cover information and events occurring in Ukraine unilaterally or incompletely, violating its integrity. The population of the state, in the conditions of hybrid war, increasingly experiences informational-psychological pressure on consciousness. All the above indicates the necessity of developing powerful mechanisms for protecting the confidentiality, accessibility, and integrity of information in Ukraine, which will prevent various encroachments on the lawful rights and interests of citizens, private and state organizations, and the state as a whole. The article highlights the connection of information security with its generic category - national security, analyzes the factors influencing the integrity, accessibility, and confidentiality of information. Attention is drawn to the necessity of developing the information culture of society, which will allow to resist adequately to the threats facing modern Ukraine in conditions of full-scale, and at the same time, hybrid war with a powerful informational component.*

***Keywords**: information, information security, information space, national security, information culture, media and information literacy, hybrid war, information law.*

***Formulas**: 0; fig.: 0, tabl.: 0, ref.: 11.*

Постановка проблеми. Упереджене і тенденційне висвітлення фактів та подій професійними засобами масової інформації, окремими популярними спікерами чи блогерами, часто є наслідком замовчування чи запізнілого повідомлення владою важливої інформації. Обговорення тих чи інших подій без достатньої інформованості доповідачів на різного роду інформаційних майданчиках, поширює суперечливу, та таку, яка часто не відповідає дійсності, інформацію, що в свою чергу породжує серед населення паніку та хаос, які шкодять національній єдності. Сучасні наукові дослідження свідчать про необхідність розробки ефективних засобів протидії поширенню дезінформації, кібератакам, руйнівним інформаційним впливам на свідомість людей різних вікових категорій та соціальних груп. В умовах гібридної війни, у якій перебуває Україна, важливо напрацювати стратегію боротьби із загрозами в інформаційній сфері, вдосконалити законодавство, особливо в частині виявлення та покарання злочинів, вчинених проти основ інформаційної безпеки людини, громадянина та держави.

Не вирішені раніше частини загальної проблеми. Безпека упродовж тисячоліть була і залишається найважливішою фундаментальною потребою людини. В умовах перебудови сучасного суспільства в напрямку його інформатизації та цифровізації, актуалізувалися дослідження з інформаційної безпеки, як необхідний крок до забезпечення гарантованих сучасній людині прав та законних інтересів. Більшість наукових праць з досліджуваної нами проблеми присвячено з'ясуванню генези, характеристик та ролі інформаційної безпеки в сучасних умовах. Такі відомі дослідники: Ю. Битяк, О. Боднар, Н. Бортник, О. Данільян, О. Дзьобань, М. Панов, Ю. Шемшученко та багато інших у своїх дослідженнях акцентують на необхідності посилення заходів боротьби з правопорушеннями, що посягають на права людини в інформаційній сфері, а саме на

приватність, свободу слова, право на інформацію, право на цифрову грамотність тощо. Інформаційну безпеку часто розглядають як необхідний елемент системи національної безпеки (В. Аніщук, А. Войціховський, І. Залевська, І. Котерлін, О. Панченко, А. Романова, М. Шевчук та ін.).

Метою статті є критичний аналіз інформаційної безпеки як детермінанти збереження української державності в умовах активної фази російсько-української війни.

Виклад основних положень. Інформаційна безпека – явище багатоаспектне, найчастіше розглядається дослідниками як одна із складових безпеки національної. Осмислення інформаційної безпеки науковцями з усього світу привело до появи дещо різних за змістом дефініцій, які надають окремі обриси тих чи інших важливих характеристик досліджуваного явища. М. Шевчук в одній із своїх праць акцентує увагу на тому, що чинне законодавство України досі не містить відповідного розгорнутого тлумачення поняття інформаційної безпеки, відмічаючи, що нормативні акти закономірно розглядають її в контексті більш загального поняття національної безпеки [11, с. 134].

Важливість національної безпеки в контексті інформаційної політики України важко переоцінити, адже сьогодні цифровий світ став чи не найбільш значимою ареною світу [8, с. 136]. Інформаційна безпека займає особливе місце у загальній системі національної безпеки держави, оскільки є елементом усіх складових системи безпеки, внаслідок чого одночасно набуває й автономного значення, – вважає О. Панченко. На думку науковця, будь-які виклики чи загрози власне національній безпеці країни безпосередньо стосуються її інформаційного чинника, а сучасна українська соціально-економічна ситуація, недосконаліть організації державної влади та громадянського суспільства створюють широкий спектр внутрішніх загроз інформаційній безпеці країни. Автор наголосив, що від інтенсивності, повноти, якості та своєчасності інформаційного обміну залежить рівень розвитку таких галузей, як оборонна промисловість, енергетика, зв'язок, наука і медицина, транспорт і виробництво в цілому [6, с. 2].

Сучасна Україна переживає важкі часи своєї історії. З-поміж усіх загроз існування та функціонування нашої держави, ми спостерігаємо цілий комплекс небезпек, пов'язаних зі збереженням критично важливої інформаційної інфраструктури, захистом державних таємниць та стратегій розвитку держави в умовах ведення проти неї як класичної конвенційної, так і гібридної війни. Важливо постійно моніторити, виявляти і знешкоджувати небезпеки для української державності в інформаційній сфері, адже стан захищеності громадян у сфері обігу інформації впливає на збереження довіри до держави, збереження престижу держави та довіри до неї, як до правової інституції, з боку міжнародних партнерів.

А. Войціховський вважає питання забезпечення інформаційної безпеки вкрай важливими для української держави на сучасному етапі її розвитку. Стратегічно визнаним пріоритетом зовнішньої політики України дослідник називає європейську інтеграцію, за якої завданням для української влади має стати розвиток ефективного діалогу з ЄС у питаннях забезпечення інформаційної безпеки. Автор наголошує також на тому, що потрібно детально вивчати практичний досвід зарубіжних країн, які вже мають організаційно-правову основу щодо забезпечення інформаційної безпеки та максимально використати їхній досвід у національній законотворчості та здійсненні дієвих заходів у зазначеній сфері [2, с. 287]. «Одним з основних висновків російсько-української війни є те, що вже зараз активно вивчається міжнародною коаліцією союзників, є докорінна зміна підходів до розуміння ролі та значення інформації», – слушно відмічає В. Швед. Якщо раніше інформація переважно сприймалась як інструмент боротьби з «туманом війни» та основа для прийняття управлінських рішень, то наразі не проходить і дня, як відповідальні спікери Збройних Сил України або українського військово-політичного керівництва не наголошують на необхідності дотримання інформаційної гігієни, критичного ставлення до наповнення інформаційного поля, необхідності боротьби, навіть на побутовому рівні,

із засиллям інформаційно-психологічних спеціальних операцій [10, с. 184].

Поширення фейків та інших елементів пропаганди важливою проблемою в умовах необхідності підтримки України її міжнародними партнерами у військовій, економічній та політичній сферах. Дезінформація, яка як правило має корупційну складову, однак досягає злочинної мети її автора. Дезінформація позбавляє проукраїнських лідерів західних держав часткової підтримки їхніх виборців, дає можливість для маніпуляцій особам, які з різних на те причин підіграють Росії. Причиною цього стає наведення в інформаційному полі зарубіжних країн великої кількості фактів, які є антиукраїнськими або суперечливими за своїм змістом, що позбавляє пересічну людину правильного розуміння про події, які відбуваються у світі.

Основні виклики і загрози для національної безпеки України, пов'язані розвитком інформаційних технологій в умовах російсько-української війни в одній із своїх наукових робіт розглядає В. Новгородський. Він намагається окреслити основні тенденції російської інформаційної кампанії, спрямованої проти України, з'ясувати напрямки російської пропаганди на окупованих територіях України, в Росії та Європі, проаналізувати ризики для демократичного світу, якщо така пропаганда матиме успіх. Нам близькою є думка автора щодо того, що інформаційна війна Росії проти України розпочалася задовго до 2014 року, а на сучасному етапі вийшла на новий виток свого розвитку і несе глобальний характер [5, с. 158]. Завданням ворожої пропаганди було і залишається дезорієнтувати не лише українське суспільство, але й європейське. Не можна недооцінювати роль інформації та інформаційних технологій в сучасному світі, позаяк разом із швидким розвитком сфери інформаційних технологій виникло безліч нових та вдосконалилися уже відомі загрози національній безпеці держави.

Аналізуючи норми національного права можна відмітити, що до основних інформаційних загроз національній безпеці законодавцем в Україні віднесено: обмеження доступу громадян до інформації, поширення за допомогою сучасних інформаційних технологій недостовірної інформації, культу насильства, жорстокості, кібертероризм, розголошення інформації, яка становить державну та іншу, передбачену законом таємницю, розповсюдження недостовірної, неповної або упередженої інформації.

Державна політика нашої держави спрямовується на захист людини і громадянина, їхнього життя, гідності, конституційних прав та свобод, на забезпечення гідних та безпечних умов життєдіяльності людини, на захист суспільства, його демократичних цінностей, умов сталого розвитку суспільства та держави, конституційного ладу, суверенітету, охорону територіальної цілісності держави, навколишнього природного середовища від надзвичайних ситуацій та техногенних катастроф тощо. Законом «Про національну безпеку України» від 21 червня 2018 року визначено, що національна безпека України – це захищеність її державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Законодавець вказує, що загрозою національній безпеці є явища, тенденції і чинники, які унеможливлюють чи ускладнюють, або можуть у майбутньому унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [7].

Національні цінності України включають широкий спектр ідеалів, які визначають унікальну ідентичність та культурний характер українського народу. До них, як правило, відносимо: незалежність і суверенітет (українська держава прагне зберігати свою незалежність та суверенітет, захищаючи свою територіальну цілісність та права свого народу), демократія та права людини (Україна віддана принципам демократії, правової держави та захисту прав і свобод своїх громадян), європейськість (тобто бажання рухатися вперед у напрямку європейської інтеграції, приймаючи європейські цінності та стандарти), патріотизм (проявляється у любові до своєї країни, гордості за її історію, культуру, мову, традиції), мир і безпека (бажання жити

в мирі та співіснувати з сусідніми країнами в атмосфері стабільності та безпеки), культурна різноманітність (включає повагу до різноманіття культур, мов, традицій та ідей, які складають в сукупності українське суспільство), сімейні цінності тощо.

Коли йдеться про інформаційну безпеку держави, зазвичай зупиняємося на її розумінні як стану, що характеризується забезпеченням захисту різного роду інформації та інформаційних ресурсів. Такий захист включає широкий спектр заходів, спрямованих на захист інформації та ресурсів від несанкціонованого (незаконного) доступу, який веде до її втрати, руйнування чи викрадення. Секретна державна інформація (військові плани, політичні стратегії, таємні дані з оборони та інші засекречені дані, розголошення яких може завдати шкоди інтересам держави), критична інфраструктура (важливі інформаційні системи, які забезпечують технологічні процеси в державі, – роботу енергетичних систем, транспортних мереж, фінансових установ тощо), персональні дані державних та громадських діячів, посадових осіб держави на різних рівнях владної вертикалі, дедалі частіше стають об'єктами злочинних посягань.

В Україні триває процес становлення системи стратегічних комунікацій. Органами державної влади України здійснено низку організаційних та практичних заходів зі зміцнення власної інституційної спроможності у сфері стратегічних комунікацій, однак не створено дієвого механізму координації і взаємодії між усіма органами державної влади, залученими до здійснення заходів із протидії загрозам в інформаційній сфері [1, с. 141]. В сучасних умовах розвитку інформаційного суспільства об'єкти критичної інфраструктури не можуть існувати без інфраструктури інформаційної (комп'ютерів і мереж, представлених, в першу чергу, системами диспетчерського управління та збору даних, взаємозалежність яких дозволяє обмінюватися інформацією та здійснювати аналіз відповідно до всіх критично важливих функцій). Здійснення далекого доступу до управління такими об'єктами на користь підвищення ефективності та скорочення витрат, відкрило критичну інфраструктуру для кіберзагроз. Нинішня геополітична арена перетворила кібератаки на критичну інфраструктуру в «кібервійну», оскільки потенціал для порушення критичної інфраструктури країни шляхом вимкнення електростанцій, руйнування нафтопроводів, навіть припинення постачання води та опалення комунальних підприємств може надати значну військову перевагу. Безперечно, що саме ці обставини в значній мірі можуть підірвати основи національної безпеки будь-якої країни світу [2, с. 286]. О. Степко вважає, що проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як розроблення теоретичних основ забезпечення безпеки інформації, створення системи органів, відповідальних за безпеку інформації, вирішення проблеми керування захистом інформації та її автоматизації, створення відповідної нормативно-правової бази, налагодження виробництва засобів захисту інформації, організацію підготовки відповідних фахівців тощо [9, с. 90]. На нашу думку, спеціальні правоохоронні органи України, як-от кіберполіція, мають бути реформовані аж до такого стану, поки у їхньому «арсеналі» будуть найкращі ІТ фахівці, необхідне нормативне та технічне забезпечення, що дозволить не лише належно розслідувати вже скоєні злочини пов'язані з обігом інформації, але й ефективно та своєчасно діяти на виявлення загроз і попереджати вчинення таких злочинів. Діяти в умовах війни необхідно негайно. Будь-яке реформування є процесом тривалим, тому, на нашу думку, для допомоги правоохоронним органам на платній основі можуть бути залучені незалежні ІТ фахівці, що потребує лише необхідної політичної волі, нормативного та фінансового забезпечення.

Застосування інформаційних технологій військовими відкрило нові можливості щодо забезпечення оборони держави зв'язком, зброєю, іншими життєво необхідними засобами інформаційно-технічного забезпечення з можливістю військового використання. Засоби вогневого ураження, наведення вогню, засоби протиповітряної обо-

рони та радіоелектронної боротьби, розвідка та контррозвідувальні операції активно використовують новітні досягнення в інформаційній сфері. Володіння інформаційними ресурсами та його захист у військовій сфері стали таким самим неодмінним атрибутом, як озброєння, боєприпаси, транспорт тощо. Виграш України в інформаційному протиборстві під час війни з Росією сприятиме досягненню її стратегічних цілей [3, с. 20]. Водночас маємо враховувати, що ворог також активно використовує розвиток інформаційних технологій задля досягнення своєї злочинної мети.

В сучасних реаліях, війна – це все менше про зброю, оперативні й тактичні зіткнення та перемоги, а все більше – про гібридність. Гібридні конфлікти передбачають наявність різних складових, в тому числі й інформаційної, яка набуває подекуди більш важливого значення, аніж військова. Наявність зброї масового знищення не гарантує державі можливість перемоги, якщо вона не забезпечена перевагою в інформаційній сфері. Така перевага створюється системою заходів щодо переведення інформаційної безпеки держави на рейки воєнного стану. І. Котерлін зазначає, що важко та навіть недоречно заперечувати роль інформації як інструменту протистояння, фактично – зброї. Інформація дозволяє вигравати у війні не зробивши жодного пострілу, шляхом формування і розпалювання внутрішніх протиріч. Така тактика є характерною для війн нового формату – гібридних, де безпосередньо військовий фактор є лише однією зі складових цілого [4, с. 145].

Вважаємо переконливим той факт, що сторона конфлікту, яка матиме перевагу в інформаційно-технічному забезпеченні, здобуде перемогу на полі бою. Свого часу знаний китайський стратег та філософ Сунь Цзи зазначав, що «полководець, який володіє інформацією про ворога, перемагає щоразу, вступаючи з ним у бій». Розуміння цінності інформації сягає давнини, а відомий в науці трактат під назвою «Мистецтво війни» є цьому гарним прикладом. Зміна тисячоліть змінила життя людей та уявлення про інформацію, а сучасний стрімкий розвиток технологій її зберігання та обміну, змінює характер військових дій в збройних конфліктах XX-XXI століть. Водночас, інформація не втрачає своєї цінності, а навпаки, набуває щоразу більшої ваги.

Висновки. В умовах війни потребуємо налагодження роботи засобів масової інформації всередині країни (захисту свободи слова, додержання принципів рівності та солідарності тощо) має вестися ефективна дипломатична та медійна робота за межами України, спрямована на знищення медійної переваги ворога. Це дозволить ефективно протидіяти російським пропагандистським інформаційно-психологічним кампаніям, інформувати громадян України та світову громадськість про реальний стан подій в державі та на фронті. Збереження державності воюючої країни вимагає, з одного боку, потужних збройних сил, а з іншого, належної роботи державного апарату, ведення владою постійного конструктивного діалогу з власними ЗМІ, населенням, задля уникнення поширенню дезінформації та дезорієнтації людей в інформаційному просторі.

Населення воюючої держави особливо вразливе до здійснення шкідливого інформаційного впливу. Швидкий розвиток подій на фронті, недостатня обізнаність громадян у військовій справі, незнання законів ведення війни, фрагментарне розуміння подій, які відбуваються в державі (в тому числі через необхідність засекречення частини інформації), не завжди своєчасна та належна комунікація між суспільством та органами державної влади, призводить до нерозуміння громадянами процесів, які відбуваються, втрати довіри до влади та солідарності з державою.

В умовах стрімкого розвитку інформаційних технологій, перед кожною правовою державою постають нові завдання. Україна, перебуваючи в активній фазі війни з Росією, через власні зусилля, за допомогою міжнародних зв’язків та міжнародної співпраці, має забезпечити власним громадянам, організаціям, незалежно від їхньої форми власності, умови для безпечного доступу, зберігання та обміну інформації, максимально запобігати порушенням прав та свобод людини в інформаційній сфері.

Література:
1. Аніщук В. Інформаційна безпека як об'єкт посягання злочинів проти основ національної безпеки України. Науковий вісник Ужгородського Національного Університету. Серія ПРАВО. Випуск 77: частина 2. 2023. С. 139-143. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2023/06/25-2.pdf (дата звернення: 26.12.2023).
2. Войціховський А.В. Інформаційна безпека як складова системи національної безпеки (міжнародний і зарубіжний досвід). Вісник Харківського національного університету імені В.Н.Каразіна. Серія «Право». Випуск 29. 2020. С. 281-288.
3. Залєвська І. І., Удренас Г. І. Інформаційна безпека України в умовах Російської військової агресії. Південноукраїнський правничий часопис. 2022. С. 20-26.
4. Котерлін І. Б. Інформаційна безпека в умовах воєнного стану у аспекті забезпечення інформаційних прав та свобод. Актуальні проблеми вітчизняної юриспруденції. №1. 2022. С. 145-150.
5. Новородовський В. Інформаційна безпека України в умовах російської агресії. Соціум. Документ. Комунікація. (9). 2020. С. 150-179. URL: https://sdc-journal.com/index.php/journal/article/view/285/228 (дата звернення: 26.12.2023).
6. Панченко О. Інформаційна складова національної безпеки. Вісник Національної академії Державної прикордонної служби України. 2019. Випуск 3. С. 1-11. URL: https://www.rdc.org.ua/download/stati/Informational-warehouse.pdf.
7. Про національну безпеку. Закон України № 2469-VIII від 21.06.2018р. зі змінами та доповненнями. URL: https://zakon.rada.gov.ua/laws/show/2469-19(дата звернення: 26.12.2023).
8. Радевич Н. Інформаційна безпека України в контексті Євроінтеграції. Міжнародний науковий вісник. №1-2 (23-24). 2021. С. 133-145.
9. Степко О. М. Аналіз головних складових інформаційної безпеки держави Науковий вісник національного авіаційного університету. Т. 1. № 3. 2011. С. 90-99. URL: file:///C:/Users/User/Downloads/alexi,+3214-8601-1-CE%20(2).pdf(дата звернення: 26.12.2023).
10. Швед В. Роль соціальних мереж у зростанні інформаційної безпеки держави. Розвиток України в умовах мілітарного впливу: соціально-правові, економічні та екологічні аспекти: Збірник матеріалів Міжнародної науково-практичної конференції (Київ, 28 березня 2023 р.). У 2-х томах. Том 1. Київ: ВАІТЕ. 2023. 464 с. URL: https://hozpravoreposit.kyiv.ua/ bitstream/handle/765432198/213/DevelopmentOfUkraine_vol1.pdf?sequence=1#page=186 (дата звернення: 26.12.2023).
11. Шевчук М. О. До питання генези поняття інформаційної безпеки як складової національної безпеки. Науковий вісник Ужгородського Національного Університету. Серія Право. Випуск 78: Частина 2. 2023. С. 134 - 139. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/285994/280058 (дата звернення: 26.12.2023).

References:
1. Anishchuk V. (2023) Informatsiina bezpeka yak obiekt posiahannia zlochyniv proty osnov natsionalnoi bezpeky Ukrainy. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia PRAVO. Vypusk 77: chastyna 2. S. 139-143.
2. Voitsikhovskyi A. V. (2020) Informatsiina bezpeka yak skladova systemy natsionalnoi bezpeky (mizhnarodnyi i zarubizhnyi dosvid). Visnyk Kharkivskoho natsionalnoho universytetu imeni V.N.Karazina. Seriia «Pravo». Vypusk 29. S. 281-288.
3. Zalievska I. I., Udrenas H. I. (2022) Informatsiina bezpeka Ukrainy v umovakh Rosiiskoi viiskovoi ahresii. Pivdennoukrainskyi pravnychyi chasopys. S. 20 – 26.
4. Koterlin I. B. (2022) Informatsiina bezpeka v umovakh voiennoho stanu u aspekti zabezpechennia informatsiinykh prav ta svobod. Aktualni problemy vitchyznianoi yurysprudentsii. №1. S. 145-150.
5. Novorodovskyi V. (2020) Informatsiina bezpeka Ukrainy v umovakh rosiiskoi ahresii. Sotsium. Dokument. Komunikatsiia. (9). S. 150-179.
6. Panchenko O. (2019) Informatsiina skladova natsionalnoi bezpeky. Visnyk Natsionalnoi akademii Derzhavnoi prykordonnoi sluzhby Ukrainy. Vypusk 3. S. 1-11.
7. Pro natsionalnu bezpeku. Zakon Ukrainy № 2469-VIII vid 21.06.2018r. zi zminamy ta dopovnenniamy.
8. Radevych N. (2021) Informatsiina bezpeka Ukrainy v konteksti Yevrointehratsii. Mizhnarodnyi naukovyi visnyk. №1-2 (23-24). S. 133-145.
9. Stepko O. M. (2011) Analiz holovnykh skladovykh informatsiinoi bezpeky derzhavy Naukovyi visnyk natsionalnoho aviatsiinoho universytetu. T. 1. № 3. S. 90-99.
10. Shved V. (2023) Rol sotsialnykh merezh u zrostanni informatsiinoi bezpeky derzhavy. Rozvytok Ukrainy v umovakh militarnoho vplyvu: sotsialno-pravovi, ekonomichni ta ekolohichni aspekty: Zbirnyk materialiv Mizhnarodnoi naukovo-praktychnoi konferentsii (Kyiv, 28 bereznia 2023 r.). U 2-kh tomakh. Tom 1. Kyiv: VAITE. 464 s.
11. Shevchuk M. O. (2023) Do pytannia henezy poniattia informatsiinoi bezpeky yak skladovoi natsionalnoi bezpeky. Naukovyi visnyk Uzhhorodskoho Natsionalnoho Universytetu. Seriia Pravo. Vypusk 78: Chastyna 2. S. 134-139.

Стаття надійшла до друку 10.02.2024 року