УДК 323:001.102-049.5-044.922(477)
DOI https://doi.org/10.32689/2523-4625-2024-3(75)-12

Віталій СІЛАЄВ
аспірант кафедри політичних наук Навчально-наукового інституту права та політології, Український державний університет імені Михайла Драгоманова,
ventilok.vs@gmail.com

Павло ГОРІНОВ
кандидат юридичних наук, доцент, директор Навчально-наукового інституту права та політології, професор кафедри правознавства та галузевих юридичних дисциплін, Український державний університет імені Михайла Драгоманова, p.v.gorinov@udu.edu.ua
ORCID*:* 0000-0002-8294-2784

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ УКРАЇНИ: ВИКЛИКИ ТА ШЛЯХИ ПОПЕРЕДЖЕННЯ

Стаття присв'ячена аналізу сучасного стану політики інформаційної безпеки в умовах цифрової трансформації України; виокремленню основних викликів і загроз інформаційної безпеки України та формулюванню шляхів протидії ним, що має особливе значення для формування системи безпеки та обороноздатності країни в умовах військової російської агресії.

Авторами сформовано наступні завдання: проаналізувати основні підходи до розуміння політики інформаційної безпеки; напрямки політики цифрової трансформації інформаційної сфери; проаналізувати основні здобутки цифрової трансформації та, виділивши інформаційні та кіберзагрози, запропонувати шляхи їх розв'язання.

Методологія дослідження базується на комплексному використанні загальнонаукових та спеціальнонаукових методів наукового пізнання, що дали можливість дослідити тематику інформаційної безпеки в умовах цифрової трансформації, яка має особливе значення для формування системи інформаційної безпеки та обороноздатності країни. Авторський підхід полягає у поєднанні використання наукових підходів, аналітичних матеріалів, досвіду діяльності державних органів і міжнародних організацій в зазначеній сфері.

Авторами акцентується увага на зростанні актуальності питання протидії інформаційним загрозам у системі заходів світової безпеки заради майбутнього.

Наукова новизна дослідження полягає в аналізі сучасного стану політики інформаційної безпеки цифрової трансформації та існуючих інформаційних викликів і кіберзагроз для визначення шляхів їх подолання. Автори наголошують, що основною метою державної політики в умовах цифрової трансформації є управління існуючими та можливими викликами і загрозами інформаційній безпеці для створення необхідних умов щодо функціонування інформаційного суспільства, вільного та безпечного кіберпростору, реалізація інформаційних прав людини і громадянина, цифрова трансформація держави і суспільства, захист національних інтересів України у сфері безпеки.

Автори наголошують на необхідності вдосконалення та розширення космічної та аерокосмічної галузі держави як базової галузі національної безпеки та оборони, а також підвищення рівня інформаційної та політико-правової освіти для протидії маніпулюванню інформацією та запобіганню кіберзагрозам.

Ключові слова*: *цифрова трансформація, політика інформаційної безпеки, інформаційні виклики війни, інформаційні атаки, інформаційна війна, Глобальний цифровий договір.

Vitalii Silaiev, Pavlo Gorinov. INFORMATION SECURITY POLICY IN THE CONDITIONS OF UKRAINE'S DIGITAL TRANSFORMATION: CHALLENGES AND WAYS OF PREVENTION

The article is devoted to the analysis of the current state of information security policy in the conditions of digital transformation of Ukraine; identifying the main challenges and threats to Ukraine's information security and formulating ways to counteract them, which is of particular importance for the formation of the country's security system and defense capability in the conditions of russian military aggression.

The authors formulated the following tasks: to analyze the main approaches to the definition of information security policy; directions of the policy of digital transformation of the information sphere; to analyze the main achievements of digital transformation and, by highlighting information and cyber threats, to propose ways to solve them.

The research methodology is based on the complex use of general scientific and special scientific methods of scientific knowledge, which made it possible to investigate the topic of information security in the conditions of digital transformation, which is of particular importance for the formation of the information security system and the country's defense capability. The author's approach consists in combining the use of scientific approaches, analytical materials, experience of the activities of state bodies and international organizations in the specified field.

The authors focus attention on the growing relevance of the issue of countering informational threats in the system of global security measures for the sake of the future.

The scientific novelty of the study consists of analyzing the current state of the information security policy of digital transformation and the existing information challenges and cyber threats to determine ways to overcome them. The authors emphasize that the main goal of state policy in the conditions of digital transformation is the management of existing and possible challenges and threats to information security to create the necessary conditions for the functioning of the information society, the functioning of a free and safe cyberspace, the realization of the informational rights of a person and a citizen, the digital transformation of the state and society, protection of national interests of Ukraine in the security sphere.

The authors emphasize the need to improve and expand the space and aerospace industry of the state as a basic industry of national security and defense, as well as to increase the level of information, and political and legal education to counter information manipulation and prevent cyber threats.

Key words: *digital transformation, information security policy, information warfare challenges, information attacks, information warfare, Global Digital Compact.*

Постановка проблеми. З розвитком інформаційних технологій, розширенням глобальних комунікаційних мереж та інтенсифікацією заходів цифрової трансформації сучасний світ увійшов у нову епоху, коли питання забезпечення інформаційної та кібербезпеки набули критичного значення для життєдіяльності соціальних інститутів, суспільства та держави. Це питання постало як на міжнародній арені, так і в рамках національних державних стратегій, що містять своє відображення в практичній діяльності урядових структур та законотворчій діяльності України. Чинне законодавство України, зокрема Конституція України, регулює питання інформаційної та кібербезпеки, визначаючи ці напрями як одні з ключових пріоритетів держави. Так, у статті 17 Конституції встановлено, що «захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є реальними функціями держави» [13], про пріоритетність питань інформаційної безпеки свідчить прийняття Стратегії інформаційної безпеки [24] та Стратегії кібербезпеки [23], Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації [21] та інші акти, де визначено пріоритетні напрямки політики інформаційної безпеки, що відповідає міжнародним стандартам і сучасним умовах цифрової трансформації суспільства та держави.

Зростаючий інтерес світової спільноти до питань інформаційної безпеки та протидії цифровим, інформаційним і кіберзагрозам значно посилився у зв'язку з викликами, що сприяють швидкому розвитку штучного інтелекту та його інтеграції у військові технології. Особливого значення це питання набуло на тлі триваючої збройної агресії російської федерації проти України, яка супроводжується масштабними інформаційними атаками, загрозами в космічному просторі та на землі.

У цьому контексті особливу увагу привертає проблема забезпечення ефективного захисту від кібератак, ураховуючи наявний технічний та технологічний потенціал сторін сучасних війн. Наприклад, нещодавні події, пов'язані з вибухами електронних пристроїв (пейджерів) у Лівані, забезпечують високий рівень можливостей для проведення кібероперацій і завдання значної шкоди супротивнику.

Усі наведені вище аспекти свідчать про нагальну потребу політики вдосконалення цифрової трансформації у сфері інформаційної безпеки як на національному, так і на міжнародному рівнях. Це зумовлено забезпеченням протидії новим викликам, пов'язаним із зростанням кіберзагроз, а також запобігання дестабілізаційним процесам у глобальній безпеці. В умовах постійного розвитку технологій і загострення геополітичної ситуації забезпечення інформаційної стійкості та кіберзахисту стає ключовим завданням як для окремих держав, так і для міжнародної спільноти.

Аналіз останніх досліджень і публікацій. Тематика інформаційної безпеки продовжує бути предметом уваги науковців різних галузей знань, серед як відзначимо напрацювання Шопіної І. М., яка в своїх працях формулює та обґрунтовує такий феномен як інформаційна безпека цифрової трансформації [30], виокремлює принципи цифрової трансформації України крізь призму досвіду Європейського Союзу [31], Войтович П. щодо дослідження організаційно-правового механізму захисту інформаційних прав людини [2], Скочиляс-Павлів О. В. щодо аналізу загроз інформаційній безпеці України в умовах правового режиму воєнного стану [25], Нашинець-Наумова А. Ю. щодо питань правового регулювання інформаційної безпеки [18], Золотар О. О., Трубін І. О. щодо класифікації загроз інформаційній безпеці [12], Карнаух А. А., Шевчук З. Ю. щодо інформаційних війн на сучасному етапі розвитку сус-

пільства [16], Куренда Л. Д. щодо забезпечення інформаційної безпеки Європейського Союзу [15], Ткачук Т. Ю. щодо дослідження державної політики у сфері забезпечення інформаційної безпеки [26], Караман О. Л. щодо розуміння інформаційно-психологічна війна на Сході України [14], Драпушко Р. Г., Горінов П. В. щодо викликів в освітній сфері, в тому числі і щодо освіти в інформаційній та політичній, правовій сферах молоді [4, 5, 6, 8], Міненко Є. щодо організаційно-правового аналізу забезпечення інформаційної безпеки як фактора суспільно-політичної стабільності [17], Тихомиров О. О. щодо забезпечення інформаційної безпеки як функції сучасної держави [27] і прав людини в інформаційній сфері [28].

Відзначимо зусилля міжнародної спільноти в формуванні політики інформаційної безпеки, а саме: рішення 79 сесії Генеральної Асамблеї ООН. 24-28 вересня 2024 року, де було ухвалено «Пакт заради майбутнього» [22], перший Міжнародний форум з кібербезпеки «Стійкість під час кібервійни», що проведено 7-8 лютого 2024 року в Києві за участі керівників відомств і міністерств України; круглий стіл, присвячений обговоренню другого законопроєкту, спрямованого на підвищення рівня кібербезпеки цифрової та критичної інфраструктури за підтримки Проєкту USAID «Кібербезпека критично важливої інфраструктури України» [19], зусилля наукової спільноти присвячені гуманітарним стандартам правових систем у сучасному світі: виклики, рішення, тенденції [3].

Мета дослідження полягає в аналізі теоретичних основ і методології вивчення сучасного стану політики інформаційної безпеки в умовах цифрової трансформації України, що має особливе значення для формування системи безпеки й обороноздатності країни в умовах військового вторгнення російської федерації.

Виклад основного матеріалу. Для досягнення мети статті використовувалися загальнонаукові та спеціальнонаукові методи наукового пізнання, що дали можливість дослідити тематику політики інформаційної безпеки в умовах цифрової трансформації.

Україна, починаючи з 2014 року, а особливо після 24 лютого 2022 року, героїчно протистоїть російській федерації у захисті своєї цілісності та безпеки у військовій, ідеологічній, інформаційній, ментальній, енергетичній, екологічній сферах тощо. Об'єктами атак російська федерація вибирає розташування сил ЗСУ, інформаційний та кіберпростір, критичну інфраструктуру, інші сфери життєдіяльності нашої держави, порушуючи норми міжнародного права та принципи ведення військових дій. Відповідно, важливим напрямком безпеки держави є забезпечення інформаційної та кібербезпеки, військової, критичної та цивільної інфраструктури в умовах цифрової трансформації усіх сфер життєдіяльності українського суспільства.

Користуючись термінами інформаційна безпека, цифрова трансформація, кібербезпека, кіберпростір, вважаємо за необхідне зупинитись на понятійному розумінні категорій та сформулювати пропозиції щодо політики забезпечення інформаційної безпеки України в умовах військового вторгнення.

Інформаційна безпека є складовим компонентом загальної проблеми інформаційного забезпечення людини, держави і суспільства. Вона орієнтована на захист значимих або вже згаданих суб'єктів інформаційних ресурсів, законних інтересів. Зміст поняття «інформаційна безпека» розкривається у практичній діяльності, наукових дослідженнях, а також нормативно-правових документах [18, с. 10].

Ураховуючи різноманітність наукових підходів до розуміння категорії «інформаційна безпека», візьмемо за основу те визначення, яке закріплене у Стратегії інформаційної безпеки, де сказано, що «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 та 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 [24].

З позиції співвідношення категорій інформаційна безпека та кібербезпека, можна сказати, що інформаційна безпека захищає всі форми інформації, як цифрові, так і фізичні. Кібербезпека, як більш складніша категорія, захищає всі форми цифрової інформації, включаючи комп'ютери, кишенькові пристрої, хмару та мережі, і є частиною системи інформаційної безпеки. Відповідно, кібербезпека – це стан захищеності даних в електронному вигляді від їх несанкціонованого використання або кримінальних дій з цими

даними, а також набір заходів для досягнення такого стану захищеності даних [20]. Україна прагне створити максимально відкритий, вільний, стабільний і безпечний кіберпростір в інтересах забезпечення прав і свобод людини, соціального, політичного і економічного розвитку держави [23].

Цифрову трансформацію за Шопіною І. М. розуміємо як «оптимізацію організації, управління, функцій та методів діяльності, інформаційної культури та інформаційної свідомості суб'єктів правовідносин за рахунок використання ними інформаційних технологій [30, с. 32]. Відзначимо, що цифрова трансформація відкриває перспективи входження України до європейського простору, що є основним пріоритетом розвитку нашої країни. Проблема забезпечення інформаційної безпеки Європейського Союзу розглядається поряд з іншими проблемами становлення інформаційного суспільства, як інформаційні загрози, кібератаки, інформаційні права тощо, що дає великі можливості для співпраці України і ЄС.

Дослідники зауважують, що «аналіз низки нормативно-правових актів та планів дій у сфері становлення інформаційного суспільства ЄС, дозволив дійти висновку про значно вужче розуміння поняття «інформаційна безпека» як щодо українського, так і до міжнародного законодавства… Отже, актуальність таких проблем, як інформаційно-технологічний дисбаланс, інформаційна ізоляція окремих регіонів, країн, а також негативний вплив інформаційних технологій, акцентується не тільки ЮНЕСКО, а й іншими міжнародними організаціями, зокрема ООН [15, с. 37]. Розуміючи значення інформаційної безпеки, Україна активно працює над подоланням інформаційного дисбалансу як в законотворчій сфері, так і в практичній площині діяльності відповідних суб'єктів. Так, ще «перед початком повномасштабної збройної агресії російської федерації наша держава знаходилася на піку розвитку цифрової трансформації процесів взаємодії громадянина і держави, а також діяльності органів публічної влади. Незважаючи на певні недоліки системи «Дія», а також єдиних і державних реєстрів (переважно пов'язаних із їх вразливістю до витоку персональних та інших даних), можна констатувати, що Україна вийшла на одне з перших місць в Європі у сфері цифрової трансформації органів публічного адміністрування. Єдина судова інформаційно-телекомунікаційна система, яка включає у тому числі й підсистему «Електронний суд», дозволила зробити великий крок уперед на шляху підвищення доступності правосуддя. Цифровізація сфери публічних послуг підвищила зручність та інклюзивність користування ними для громадян, а також сприяла зниженню корупційних ризиків у найбільш чутливих сферах правовідносин [30, с. 32]. До цього переліку об'єктів цифровізації, слід добавити нові цифрові продукти, які були створені в час військового протистояння, а саме, «Армія+», «Резерв+» та у майбутньому чекаємо запуск «Ветеран+». Так, в «Резерв+» за даними Міністерства оборони України майже 3,5 млн українців отримали електронний військово-обліковий документ.

Станом на вересень 2024 року Україна посіла п'яте місце у світі за рівнем розвитку цифрових державних послуг та ввійшла у топ-25 рейтингу країн світу за рівнем кібербезпеки. Це глобальний індекс, який вимірює готовність країн запобігати кіберзагрозам і відповідати на інциденти. Окремо відзначимо, що м. Київ увійшов у топ-15 найкращих міст світу за рівнем цифровізації і розвитку електронних сервісів. Проте, слід зауважити, що «існує потреба у належному правовому регулюванні використання програмного й інформаційно-технічного забезпечення критичної інфраструктури міст і сіл, медичної та гуманітарної сфер і навчання навиків користування інформаційними ресурсами, критичного мислення й інформаційної гігієни [8, с. 34].

Сьогодні українські фахівці працюють спільно з міжнародними партнерами над процесом цифрової трансформації державних органів. Так, спільно з партнерами в рамках USAID Cybersecurity Activity 17 вересня 2024 року відбувся круглий стіл, присвячений обговоренню другого законопроєкту, спрямованого на підвищення рівня кібербезпеки цифрової та критичної інфраструктури держави. Законопроєкт імплементує ключову Директиву (ЄС) 2022/2555, яка відкриває двері для інтеграції України в Єдиний цифровий ринок ЄС, що стане важливим кроком у контексті вступу України до Європейського Союзу [19].

Труднощі забезпечення цифрового процесу трансформації країни завдають гібридні військові дії, що тривають у світі та несуть ризики для системи електронних засобів і відповідних інформаційних продуктів, так як в світі «зараз триває перша кібервійна», активні дії якої проходять на території різних державних та в різних формах прояву. Так, журнал «The wall street journal» піднімає питання кіберзагроз, які існують для цивільної авіації, адже «сотні щоденних рейсів у всьому світі стикаються з підробкою GPS, небезпекою, що створює нові ризики для пілотів і пасажи-

рів [9]. Такі загрози відповідають розумінню інформаційної війни, сформульованої Карнаух А. А., Шевчук З. Ю. «як цілісної стратегії, обумовлену всезростаючою значимістю і цінністю інформації в питаннях керування всіма сферами держави і людської життєдіяльності з використанням відкритих та прихованих інформаційних впливів [16, с. 99].

З метою координації роботи в цьому напрямку, 22 вересня 2024 року, в рамках роботи 79 сесії Генеральної Асамблеї ООН було ухвалено «Пакт заради майбутнього», який включає Глобальний цифровий договір і Декларацію про майбутні покоління. У цьому документі встановлюється зобов'язання діяти «колективно для підтримки й відновлення міжнародного миру і безпеки на суші, морі, в космосі, у кіберпросторі та в інших нових сферах» [22]. Погоджуємось, що роль України є важливою у процесах захисту кіберпростору на світовому рівні, тому, на думку В. Зеленського: «Україна, має відновити лідерство та статус провідної аерокосмічної держави [29], адже космос в XXI столітті стає ареною протистояння між основними космічними державами світу та є джерелом нових інформаційних і кіберзагроз.

Інформаційна безпека суспільства повинна забезпечувати безпеку індивідуальної, групової і масової свідомості громадян у рамках інформаційних загроз, які виражаються в інформаційно-психологічному впливі [25]. Це проявляється в тому, що під час війни спостерігаємо паралельно з військовими діями, ментальні, або психологічні війни. Особливістю їх є те, що, на думку фахівців, «інформаційно-психологічний вплив на населення спрямований на емоційну сферу свідомості. …. об'єкт впливу або приймає готові установки, або не приймає, приймає цілком або частково. Інформаційно-психологічний вплив на емоційну сферу свідомості включає нецілеспрямоване сприйняття і запам'ятовування і характеризується різко зниженим рівнем усвідомлення змісту впливу. Осмислення отриманої інформації відбувається пізніше, при більш високій пізнавальній активності об'єкта [26]. Отже, одним з напрямків забезпечення інформаційної безпеки є формування такого стану інформаційно-психологічної безпеки, який би унеможливлював завдання шкоди маніпуляціями, дезінформацією, пропагандою ворога й іншими проявами інформаційних атак.

Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини (як громадян, так і державних посадових осіб) та суспільства, пов'язаних передусім із маніпулюванням свідомістю з різною метою, зокрема терористичною, і поширенням суспільно небезпечної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо) [27, с. 70]. Таким чином, вважаємо, що є потреба посилення роботи з протидії дезінформації та іншими негативними явищами, шляхом формування навиків критичного мислення й аналітики, адже аналітичні навики роботи з інформацією є одним із способів протидії дезінформації та маніпулювання нею.

Оскільки інформаційна безпека є важливим елементом національної безпеки, більшість країн усього світу приділяють цьому напрямку безпеки особливу увагу та розробляють комплексні заходи для її забезпечення [17, с. 80]. Так, в Стратегії кібербезпеки [24] передбачено, що для досягнення цілей у сфері кібербезпеки «в Україні будуть проведені наукові дослідження у сфері кібербезпеки, реформовано систему підготовки та підвищення кваліфікації кадрів, а також розгорнуто навчальні програми, курси, тренінги з кіберзахисту для всіх верств населення шляхом розроблення Загальнонаціональної програми кіберграмотності, спрямованої на підвищення рівня цифрової грамотності населення України, зокрема, шляхом включення питань стосовно цифрових навичок, кіберобізнаності щодо сучасних кіберзагроз та протидії ним до навчальних програм загальної середньої, професійної (професійно-технічної), фахової передвищої та вищої освіти. Ми повністю підтримуємо подібні ініціативи, проте вважаємо, що такі курси мають бути розроблені у поєднанні з правовою та політичною освітою, що рекомендували наступні автори у своїх працях [4, 5, 6, 7, 8]. Подібної позиції притримується і Войтович П., який вважає за доцільне поширення «розвитку освітніх програм, що сприятимуть підвищенню правової обізнаності громадян в аспекті інформаційних прав [2, с. 36] та Тихомиров О. О. у своїх працях [27, 28]. Погоджуємось із усіма авторами про важливість інформаційної освіти, проте, вважаємо, що лише комплексне поєднання вищевказаних напрямків освіти дасть можливість належним чином відповідати на нові виклики інформаційного, безпекового, політичного і правового характеру.

Відзначимо позитивний процес у створенні серії освітніх програм з кіберзахисту Офісом Генерального прокурора, Міністерством цифрової трансформації та платформою «Дія. Освіта». У межах цих програм фахівці нададуть рекомендації, як розпіз-

нати кіберзлочини та не стати їх жертвою, а також, що робити, якщо людина постраждала [1], але цей курс бажано розширити, зробити комплексним і запровадити в усіх навчальних закладах України.

Висновки. Проведене дослідження дозволяє стверджувати, що безпека сучасного суспільства значною мірою залежить від стабільного функціонування інформаційної інфраструктури. Процес цифрової трансформації адекватно відповідає сучасній інформаційній та кіберзагрозі як на глобальному рівні, так і в Україні. Цифрова трансформація інформаційної безпеки інтегрується в міжнародний процес, спрямований на посилення інформаційних комунікацій, розробку стратегій і концепцій, а також забезпечення безпеки й адаптацію політичних рішень в умовах воєнного стану в Україні.

Погоджуємось, що «інформаційна безпека цифрової трансформації – це ідеальна модель позбавленого інформаційних загроз середовища, в якому динамічно відбувається впровадження інформаційних (цифрових) технологій у всі сфери функціонування та життєдіяльності фізичних і юридичних осіб з метою найбільш повної реалізації ними своїх інформаційних та інших прав, свобод та інтересів [30, с. 34].

Вважаємо, що існує потреба прийняття політичних рішень та нормативно-правового забезпечення у сфері цифрової трансформації як способу протидії інформаційним загрозам в умовах воєнної агресії російської федерації. Отже, можемо констатувати, що Україна, вдосконалюючи законодавство в сфері інформаційної безпеки, тим самим працює в напрямку руху до Європейського Союзу щодо «побудови стійкого цифрового суспільства, заснованого на людино центризмі» [31, с. 34].

Основною метою державної політики в умовах цифрової трансформації є управління існуючими і можливими викликами та загрозами інформаційної безпеки з метою створення необхідних умов для функціонування інформаційного суспільства, вільного та безпечного кіберпростору, реалізації інформаційних прав людини та громадянина, цифрової трансформації держави та суспільства, захисту національних інтересів України у безпековій сфері.

З огляду на значний потенціал України в космічних і суміжних високотехнологічних галузях, вбачається необхідним підтримати на належному рівні розвиток технічних та інформаційних секторів країни. Особливо ефективним є вдосконалення та розширення космічної та аерокосмічної галузей як ключових компонентів національної безпеки та оборони. Очікується, що подальші наукові дослідження в цих сферах сприятимуть глибшому розумінню проблематики захисту національного інформаційного простору та боротьби з кіберзлочинністю, а також нададуть важливі висновки та рекомендації для зміцнення інформаційної стійкості держави.

Література:

1.В Україні запустили цикл освітніх програм з кібербезпеки. URL: https://tvoemisto.tv/news/v_ukraini_zapustyly_tsykl_osvitnih_program_z_kiberbezpeky_167065.html

2.Войтович П. Становлення організаційно-правового механізму захисту інформаційних прав людини. *Наукові праці Міжрегіональної академії управління персоналом*. 2024. Вип. 2. С. 32–37.

3.Гуманітарні стандарти правових систем у сучасному світі: виклики, рішення, тенденції: матеріали Міжнародного науково-практичного конгресу у 2 частинах. Частина 1 (м. Запоріжжя, 16 травня 2024 року) / за заг. ред. Т. О. Коломоєць. Запоріжжя: ЗНУ, 2024. 255 с.

4.Горінов П. В. Правова освіта в умовах дії воєнного стану в Україні. *Актуальні проблеми вітчизняної юриспруденції.* 2023, № 1. URL: http://apnl.dnu.in.ua/6_2022/1.pdf. (дата звернення: 25.09.2024).

5.Horinov P., Mereniuk K. Military law in Ukraine: future prospects for development. Futurity Economics & Law, 2022. 2(3), p. 18–27. https://doi.org/10.57125/FEL.2022.09.25.03

6.Драпушко Р. Г., Горінов П. В. Сучасні виклики і загрози правової культури молоді. Аналітично-порівняльне правознавство. 2021. № 4. С. 18–22.

7.Драпушко Р. Г., Горінов П. В. Роль викладання юридичних дисциплін у процесі модернізації системи освіти в Україні в умовах безпекових викликів. Модернізація педагогічної освіти у глобальному вимірі безпеки соціально-турбулентного світу. 2023. № 1. С. 188–191.

8.Драпушко Р. Г., Горінов П. В., Філик Н. В. Шляхи реформування системи охорони інтелектуальної власності в умовах воєнних загроз. *Ірпінський юридичний часопис*: науковий журнал. 2022. Вип. 1 (8). С. 32–40.

9.Electronic Warfare Spooks Airlines, Pilots and Air-Safety Officials. The wall street journal. Updated Sept. 23, 2024 URL: https://www.wsj.com/business/airlines/electronic-warfare-spooks-airlines-pilots-and-air-safety-officials-60959bbd?mod=hp_lead_pos7 (дата звернення: 25.09.2024).

10. Зараз триває перша у світі кібервійна. Михайло Федоров на Міжнародному форумі з кібербезпеки. URL: https://reserveplus.mod.gov.ua/guide/ (дата звернення: 25.09.2024).

11. Золотар О. О., Трубін І. О. Класифікація загроз інформаційній безпеці. *Інформація і право*, № 3(9) / 2013. С.105–112.

12. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 25.09.2024).

13. Караман О. Л. Інформаційно-психологічна війна на сході України: сутність та механізми / О. Л. Караман. Соціологія та соціальна робота в умовах національних та регіональних викликів: матеріали доповідей та повідомлень міжнародної науково-практичної конференції. Ужгород : ТОВ «РІК-У». 2019. С. 36–37.

14. Куренда Л. Д. Окремі аспекти забезпечення інформаційної безпеки Європейського Союзу *Правова інформатика*. 2011. № 3-4(31). С. 36–42.

15. Карнаух А. А., Шевчук З. Ю. Інформаційна війна на сучасному етапі розвитку суспільства. *Науковий часопис НПУ імені М. П. Драгоманова: Економіка і право*. 2015. Вип. 29. С. 98–103.

16. Міненко Є. Організаційно-правовий аналіз забезпечення інформаційної безпеки як фактор суспільно-політичної стабільності. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 22. Політичні науки та методика викладання соціально-політичних дисциплін.* 2023. № 33. С. 76–84. URL: https://enpuir.npu.edu.ua/bitstream/handle/123456789/43809/Minenko-76-84.pdf?sequence=1&isAllowed=y

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

18. Наближення кібербезпекового законодавства України до ЄС: друга частина експертного обговорення. URL: https://cspa.digital/roundtable-1709/?fbclid=IwY2xjawFg1MNleHRuA2FlbQIxMAABHdS42INy_LDaCidk2wocOhirc-Vtej7wTZu5GnzUks9mrFasrZdzxEvPcQ_aem_e7YGOwqPl7J8bJ--DxPy6Q (дата звернення: 25.09.2024).

19. Основи кібербезпеки. URL: https://moz.gov.ua/uk/osnovi-kiberbezpeki-2 (дата звернення: 25.09.2024).

20. Про схвалення Стратегії здійснення цифрового розвитку, цифрових трансформацій і цифровізації системи управління державними фінансами на період до 2025 року та затвердження плану заходів щодо її реалізації від 7 квітня 2023 року. URL: https://ips.ligazakon.net/document/view (дата звернення: 25.09.2024).

21. Summit of the Future. Pact for the Future that includes a Global Digital Compact and a Declaration on Future Generations. URL: https://www.un.org/en/summit-of-the-future (дата звернення: 25.09.2024).

22. Стратегія кібербезпеки України, затверджена Указом Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 25.09.2024).

23. Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#Text (дата звернення: 25.09.2024).

24. Скочиляс-Павлів О. В. Сучасні загрози інформаційній безпеці України в умовах правового режиму воєнного стану. URL: http://lsej.org.ua/9_2023/65.pdf (дата звернення: 25.09.2024).

25. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Інформаційна безпека в сучасному світі та її вплив на конституційний лад в Україні: теорія й практика: матеріали всеукраїнської конференції (м. Івано-Франківськ, 20 червня 2019 року) / упорядник В. І. Розвадовський. Івано-Франківськ: ВДНЗ «Прикарпатський національний університет імені Василя Стефаника» 2019. 116 с.

26. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави: моногр. / О. О. Тихомиров; заг. ред. Р. А. Калюжний. − Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.

27. Тихомиров О. О. Права людини: інформаційний вимір: монографія. Одеса : Вид-во «Юридика», 2023. 304 с.

28. Україна має відновити лідерство та статус провідної аерокосмічної держави, тому треба змінювати підхід до фінансування космічної галузі – Володимир Зеленський. URL: https://www.president.gov.ua/news/ukrayina-maye-vidnoviti-liderstvo-ta-status-providnoyi-aerok-67941 (дата звернення: 25.09.2024).

29. Шопіна І. М. Інформаційна безпека цифрової трансформації. *Науковий вісник Львівського державного університету внутрішніх справ*. Серія юридична 2023. № 1. С. 29–35.

30. Шопіна І. М. Принципи цифрової трансформації України крізь призму досвіду Європейського Союзу. *Південноукраїнський правничий часопис*. 2022. № 4, ч. 3. С. 29–34.