УДК 342.351.746.1
DOI https://doi.org/10.24144/2788-6018.2023.06.85

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ ТА ЗАГРОЗ З БОКУ РФ

Подорожна Т.С.,
докторка юридичних наук, професорка,
професорка кафедри теорії держави та права
Львівського торговельно-економічного університету
ORCID ID: 0000-0003-0502-950X

Подорожна Т.С. Забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ.

У статті досліджено питання забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ. Зазначено, що стійкість функціонування інститутів публічної влади, збереження правопорядку є необхідною передумовою дотримання прав людини. В умовах розвитку технологій забезпечення інформаційної безпеки є однією з найважливіших гарантій прав людини. В основі таких гарантій лежить дотримання принципів конфіденційності, цілісності та доступності інформації й інформаційних систем. Для забезпечення інформаційної безпеки особистості виробляються спеціальні правові засаді захисту права на недоторканність приватного життя, а також додаткові механізми його захисту, пов'язані із встановленням специфічних вимог у сфері збору й обробки особистої інформації. Для забезпечення національної безпеки та інформаційної безпеки держави як однієї з її складових найважливішою гарантією прав людини слугує дотримання принципу пропорційності при їх обмеженні. Більшість держав відреагувало на загрози національній безпеці, що зросли останнім часом, розширивши повноваження органів влади з доступу до особистої інформації, її збору та обробки, які зараз не обмежені якимись окремими категоріями інформації. При цьому в різних державах підходи до забезпечення пропорційності вживаних заходів щодо забезпечення національної безпеки також можуть відрізнятися. Наголошено, що дії сучасних терористів виходять за межі елементарних гуманітарних принципів (у цьому контексті про РФ можна говорити як найбільш небезпечного терориста сучасного періоду розвитку людства). Відбувається зневажання основ людяності. В умовах такої боротьби важко закликати до поваги прав людини, застосовувати цей посил до тих, хто повністю його ігнорує. Практично щодня потужним кібератакам із застосуванням просунутих інформаційних технологій піддаються державні установи, ЗМІ, об'єкти критичної інфраструктури, система життєзабезпечення. Усе це – частина скоординованої інформаційної агресії проти України. Зроблено висновок, що потрібна особлива увага до завдань захисту відповідних ресурсів органів виконавчої влади, включно з Міністерством закордонних справ України. Потрібно постійно удосконалювати вжиті з цією метою заходи, налагодити повсякденний контроль виконання відповідних доручень Кабінету Міністрів України. Підкреслено, що в умовах геополітичної нестабільності та трансформації світового порядку сучасні кібератаки, які вирізняються нестандартними методами, способами та засобами їх вчинення, потребують на законодавчому рівні оперативності роботи із запобігання та недопущення деструктивного впливу на вітчизняні інформаційні ресурси й інформаційну інфраструктуру державного та приватного сектору.

Ключові слова: права людини, безпека, право на безпеку, право на інформаційну безпеку, інформація, інформаційно-правова культура, інтернет, соціальні мережі.

Podorozhna T.S. Ensuring information security of Ukraine in the conditions of modern challenges and threats from the Russian Federation.

The article examines the issue of ensuring information security of Ukraine in the conditions of modern challenges and threats from the Russian Federation. It is noted that the stability of the functioning of institutions of public authority, the preservation of law and order is a necessary prerequisite for the observance of human rights. In the conditions of technological development, ensuring information security is one of the most important guarantees of human rights. The basis of such guarantees is the observance of the principles of confidentiality, integrity and availability of information and information systems. In order to ensure the information security of the individual, special legal frameworks for the protection of the right to the inviolability of private life are being developed, as well as additional mechanisms for its protection related to the establishment of specific

requirements in the field of collection and processing of personal information. In order to ensure national security and information security of the state as one of its components, the most important guarantee of human rights is the observance of the principle of proportionality when restricting them. Most states have responded to the threats to national security that have grown recently by expanding the authorities' powers to access, collect and process personal information, which are now not limited to any particular categories of information. At the same time, approaches to ensuring the proportionality of measures taken to ensure national security may also differ in different states. It is emphasized that the actions of modern terrorists go beyond elementary humanitarian principles (in this context, we can talk about the Russian Federation as the most dangerous terrorist of the modern period of human development). There is contempt for the basics of humanity. In the conditions of such a struggle, it is difficult to call for respect for human rights, to apply this message to those who completely ignore it. Almost every day, state institutions, mass media, critical infrastructure objects, and the life support system are exposed to powerful cyber attacks using advanced information technologies. All this is part of a coordinated informational aggression against Ukraine. It was concluded that special attention should be paid to the tasks of protecting the relevant resources of the executive authorities, including the Ministry of Foreign Affairs of Ukraine. It is necessary to constantly improve the measures taken for this purpose, to establish day-to-day control of the execution of relevant assignments of the Cabinet of Ministers of Ukraine. It is emphasized that in the conditions of geopolitical instability and transformation of the world order, modern cyber-attacks, which are characterized by non-standard methods, methods and means of their perpetration, require, at the legislative level, prompt work to prevent and prevent a destructive impact on domestic information resources and the information infrastructure of the public and private sector.

Key words: human rights, security, the right to security, the right to information security, information, informational and legal culture, the Internet, social networks.

Актуальність теми дослідження. Права людини є фундаментом сучасної правової держави. На нинішньому етапі розвитку захист прав людини набуває особливого характеру. Удосконалення інформаційно-комунікаційних технологій супроводжується розширенням можливостей їх недобросовісного використання, що створює загрози інформаційній безпеці та може призводити до порушень прав людини. В Україні поняття «безпека», «інформаційна безпека» та «національна безпека» розкриваються через «стан захищеності життєво важливих інтересів особистості, суспільства та держави. Інформація є одним з головних економічних і політичних ресурсів сучасного суспільства. Вона розширює коло різних способів її використання в освітніх, соціальних, економічних і культурних цілях, а також у сфері забезпечення законності та правопорядку, в інших суспільно значущих цілях. Інформаційна безпека в цьому випадку визначається як стан захищеності національних інтересів Української держави в інформаційній сфері, що складається зі сукупності збалансованих інтересів особи, суспільства та держави, від внутрішніх і зовнішніх загроз.

Вплив сучасних інформаційно-комунікаційних технологій проявляється насамперед у сфері особистих прав, серед яких особливе місце посідає право на недоторканність приватного життя. Без інформаційної безпеки не може бути недоторканності приватного життя. Тому забезпечення інформаційної безпеки особистості становить основу правового захисту недоторканності приватного життя. З розвитком технологій істотно збільшуються обсяги та швидкість обміну інформацією, розширюється спектр можливих способів її збирання, обробки, надання та поширення. У підсумку шкода, яка може бути завдана індивідові внаслідок розкриття тієї чи іншої інформації або у зв'язку зі збереженням її в таємниці, також зростає. Утім, держава завжди оперативніше реагує на можливості, які надають нові інформаційно-комунікаційні технології для захисту публічних інтересів, ніж приватних. Це пов'язано з тим, що стійкість функціонування інститутів публічної влади, збереження правопорядку є необхідною передумовою дотримання прав людини. Більшість держав відреагувало на загрози національній безпеці, що зросли останнім часом, розширивши повноваження органів влади з доступу до особистої інформації, її збору та обробки, які зараз не обмежені якимись окремими категоріями інформації. При цьому в різних державах підходи до забезпечення пропорційності вживаних заходів щодо забезпечення національної безпеки також можуть відрізнятися.

У державах з демократичними правовими режимами зазвичай встановлено пріоритет прав людини над забезпеченням національної безпеки. Такий пріоритет виявляється в тому, що заходи щодо забезпечення національної безпеки, пов'язані зі збором та обробкою відповідної інформації, приймаються при дотриманні спеціальної процедури, яка забезпечує їх пропорційність загрозам, що виникають. В основі цього підходу лежать положення Конвенції 1950 року, в якій визначено умови обмеження прав людини на приватну недоторканність життя – «встановлення обмеження лише законом» та «необхідність у демократичному суспільстві» [1].

Отже, в умовах розвитку технологій забезпечення інформаційної безпеки є однією з найважливіших гарантій прав людини. В основі таких гарантій лежить дотримання принципів конфіденційності, цілісності та доступності інформації й інформаційних систем. Для забезпечення інформаційної безпеки особистості виробляються спеціальні правові засаді захисту права на недоторканність приватного життя, а також додаткові механізми його захисту, пов'язані із встановленням специфічних вимог у сфері збору й обробки особистої інформації. Для забезпечення національної безпеки та інформаційної безпеки держави як однієї з її складових найважливішою гарантією прав людини слугує дотримання принципу пропорційності при їх обмеженні. Загалом реалізація цього принципу та механізмів захисту прав людини при забезпеченні інформаційної безпеки може набувати різних форм, які залежать від правових традицій та політичного режиму держави.

Ступінь наукової розробки. Проблеми правового забезпечення інформаційної безпеки держави в умовах нових викликів і загроз найбільше розроблено в наукових працях О. Барабаш, І. Валюшко, А. Войціховського, М. Гаврильців, Д. Бєлова, М. Дмитренко, Т. Кірієнко, В. Нестеровича, Н. Пархоменко, Н. Оніщенко, Т. Ткачука, О. Шевчука та інших провідних вітчизняних учених у цій галузі. Проведений аналіз засвідчує, що у вітчизняній науці накопичено істотний багаж знань з окремих аспектів інформаційної безпеки.

Мета статті. Визначення питання забезпечення інформаційної безпеки України в умовах сучасних викликів та загроз з боку РФ.

Методологічну основу дослідження становить міждисциплінарний підхід до дослідження проблеми, що використовує положення філософії, юриспруденції, соціології, політології, військової науки та інших галузей наукового пізнання. У процесі дослідження проблем правового забезпечення інформаційної безпеки застосовувалися загальнонаукові методи (абстрагування, аналіз, синтез, аналогія, індукція, дедукція, моделювання).

Виклад матеріалу. Для сучасного періоду характерний значний прогрес у розвитку інформаційно-комунікаційних технологій та інформаційної інфраструктури загалом. Водночас подекуди спостерігаємо загострення суспільних відносин внутрішньодержавного чи транскордонного рівня під час їх активного використання. Зокрема, йдеться про порушення права на приватність, захист персональних даних, інформаційні конфлікти та інформаційні війни тощо [2, с. 136]. Сучасні цифрові технології, поєднуючи в собі конвергентність, наскрізний і проривний характер для розвитку суспільства та держави, не тільки створюють безмежні можливості, а й формують нові виклики і загрози безпеці в процесі їх впровадження та використання. При цьому нині забезпечення національної безпеки характеризується як комплексна система, детермінована дією різноманітних чинників і загроз [3]. Умови цифрової трансформації внаслідок бурхливого розвитку цифрових технологій, які від самого початку передбачали позитивний вплив на всі сфери життєдіяльності за умови адекватного використання досягнень науково-технічного прогресу, водночас не тільки можуть стати ефективним інструментом творчого перетворення суспільних відносин, а й приховують у собі певні ризики. Так, останніми роками зафіксовано значне збільшення кількості злочинів, вчинених з використанням комп'ютерних технологій.

Досліджуючи статистичні дані, зауважимо, що, до прикладу, за перше півріччя 2021 року у сфері протидії інформаційним загрозам в Україні було розпочато 21 кримінальне провадження за ст. 109 і ст. 110 Кримінального кодексу України; оголошено підозру 19 особам; заборонено в'їзд в Україну понад 50 іноземним громадянам; заблоковано вісім ботоферм загальною кількістю понад 35 тисяч акаунтів; припинено діяльність 16 інтернет-агітаторів; проведено понад 180 профілактичних заходів; заблоковано 58 вебресурсів, на яких поширювався фейковий та деструктивний контент [4]. Статистичні дані свідчать, що кількість кібератак щороку збільшується, тож і завдана шкода вітчизняній інформаційній інфраструктурі також зростає. За різними даними, кількість інформаційних атак з кожним роком збільшується приблизно на 6,5 % порівняно з попереднім.

Дискусії про співвідношення свободи у цифровому просторі та забезпечення безпеки актуалізуються і у зв'язку з поширенням такого негативного явища як теракти. Сама постановка проблеми не нова. Точку відліку можна визначити 11 вересня 2001 року, коли масштабний напад на торговий центр у Нью-Йорку призвів до модернізації антитерористичного законодавства і США, і більшості провідних країн світу. У США протягом місяця після атаки було розроблено та прийнято Патріотичний акт, який вніс вагомі зміни до багатьох законодавчих актів, де центральне місце приділялося запровадженню масштабних обмежень права на недоторканність приватного життя. На знак підтримки діяльності США та підтвердження союзницьких зобов'язань щодо НАТО в країнах Західної Європи відбулась активна зміна законодавчих актів, присвячених протидії тероризму:

– Німеччина, січень 2002 року – Закон про боротьбу з міжнародним тероризмом – Gesetz zur Bekämpfung des internationalen Terrorismus (TerrorBekämpfG) [5];

– Італія – Закон від 15 грудня 2001 року № 438 «Про невідкладні заходи з метою боротьби з міжнародним тероризмом» [6];

– Великобританія, грудень 2001 року – Акт про боротьбу з тероризмом, злочинність та безпеку [7].

Антитерористичне законодавство почало проникати у всі сфери життя, завдяки чому з'явився новий термін – «сек'юритизація» (концепція, в рамках якої питання у сфері міжнародної безпеки розглядаються крізь призму політичного конструктивізму і класичного реалізму) [8]. Така тенденція виявилась досить швидко, оскільки ще 2004 року генеральний секретар Міжнародної комісії юристів Ніколас Хоуен висловив таку думку: «Контртерористичні заходи у всьому світі ставлять під сумнів усі наші базові уявлення про верховенство закону та права людини» [9].

У згаданих законодавчих актах на чільне місце в предметі регулювання ставиться саме безпека. Це поняття, незважаючи на свою ясність, потребує уточнення. До того ж особливого значення набуває не саме визначення безпеки, а його тлумачення при співвідношенні з іншими конституційними цінностями. При співвідношенні прав людини, свободи у цифровому просторі та забезпечення безпеки виникає потреба балансу цінностей. Пошук балансу – найбільш складне питання, особливо, коли потреба в ньому виникає у складних процесах, таких як боротьба з тероризмом у цифровому просторі.

Загалом інтернет потребує неординарних підходів щодо правового режиму. З одного боку, безпека суспільства – справедлива вимога, яку громадяни висувають до держави. Адже не держава – основний бенефіціар безпеки, а суспільство та громадяни. Якщо виходити з іншого підходу, тоді відбувається протиставлення держави суспільству та особистості. XXI ст. відрізняється особливим ставленням до права і держави, де нав'язування ідеї про якусь божественну природу державної влади та її специфічне призначення навряд чи знайде відгук більшості населення (тим паче молоді). Можна вважати таке ставлення негативним, але його підтверджують соціологічні та політологічні дослідження. Це означає, що його варто враховувати під час побудови правової політики та пояснення будь-якої законотворчої ініціативи. Відбувається зміна принципів взаємовідносин, де саме інтернет відіграє вагому роль, розсуваючи простір, створюючи альтернативну реальність, пропонуючи хмарні технології та багато іншого. Отже, при поясненні новел у правовому регулюванні соціальних мереж потрібне зрозуміле, доступне, об'єктивне пояснення їх необхідності для забезпечення безпеки користувачів як повноправних членів громадянського суспільства. Держава – інструмент у досягненні заявленого результату. Це складний шлях, який не має простих рішень. Однак інший шлях неможливий, якщо держава й суспільство бажають рухатись вперед у своєму цивілізованому розвитку.

Іноземний дослідник К. Сурлей наголошує: «Коли держави не можуть знайти баланс між правами людини та безпекою в контексті боротьби з тероризмом, вони ризикують нашкодити тим самим правам» [10]. До того ж побічною метою будь-якої терористичної організації є провокування держави на непропорційні заходи протидії. Піднімаючи ціну боротьби, виграє лише деструктивний елемент, створюючи основу для пропаганди та вербування більшої кількості прихильників. У всіх міжнародних документах держави закликаються до дотримання базових зобов'язань щодо дотримання прав людини. Відмова від цього посилу призводить до дискредитації благих засад, закладених у боротьбі з тероризмом. Саме підвищення ролі прав людини має привести до ефективної боротьби з тероризмом, який у міжнародних актах однозначно розуміється як акт агресії проти прав людини [11].

Водночас не можна не відзначити, що дії сучасних терористів виходять за межі елементарних гуманітарних принципів (у цьому контексті про РФ можна говорити як найбільш небезпечного терориста сучасного періоду розвитку людства). Відбувається зневажання основ людяності. В умовах такої боротьби важко закликати до поваги прав людини, застосовувати цей посил до тих, хто повністю його ігнорує. У зв'язку із цим представники правоохоронних органів (і тут практично немає винятків країн світу) зауважують, що загальний дискурс про верховенство права і свободи людини та громадянина розрахований на ідеальну ситуацію [12]. Тероризм (особливо в сучасному вигляді) є винятком. У цьому разі дуже складно наполягати на безумовному дотриманні гуманітарних основ співжиття. До того ж не можна доводити юридичні формули до абсурду, коли дотримання базового змісту основних прав людини підмінюється вишукуванням нюансів, що мають мало спільного зі самим первинним правом. Завдяки цій тенденції держави щораз активніше наполягають на суверенних засадах забезпечення безпеки. Права людини дедалі частіше перетворюються на національну (а не міжнародну) проблему. Такий підхід неминуче призведе до самоізоляції, що загрожує негативними наслідками для всієї правової системи.

Водночас можемо констатувати, що органи публічної влади адаптуються до нових умов роботи в IT-середовищі з урахуванням нових великих викликів, загроз і ризиків. Посилення протиправного впливу на інформаційні ресурси в системі публічного управління зажадали вжиття додаткових заходів щодо забезпечення інформаційної безпеки. Адже поява нових інформаційних технологій

тягне за собою зміну звичних парадигм, визначає нові правила щодо використання інформаційних систем, надавши при цьому чергового імпульсу на перехід у цифрову сферу діяльності публічних органів і недержавних організацій.

Практично щодня потужним кібератакам із застосуванням просунутих інформаційних технологій піддаються державні установи, ЗМІ, об'єкти критичної інфраструктури, система життєзабезпечення. Усе це – частина скоординованої інформаційної агресії проти України. Потрібна особлива увага до завдань захисту відповідних ресурсів органів виконавчої влади, включно з Міністерством закордонних справ України. Потрібно постійно удосконалювати вжиті з цією метою заходи, налагодити повсякденний контроль виконання відповідних доручень Кабінету Міністрів України.

Вважаємо, що в умовах геополітичної нестабільності та трансформації світового порядку сучасні кібератаки, які вирізняються нестандартними методами, способами та засобами їх вчинення, потребують на законодавчому рівні оперативності роботи із запобігання та недопущення деструктивного впливу на вітчизняні інформаційні ресурси й інформаційну інфраструктуру державного та приватного сектору.

Сьогодні стан інформаційної безпеки викликає певне занепокоєння з огляду на систематичні атаки, що здійснюються з метою дестабілізації традиційних суспільних відносин в окремих регіонах світу, а також поширення недостовірної інформації для просування власних національних інтересів у військово-політичних та інших ворожих цілях [13]. Активізовуються процеси поширення недостовірної інформації «недружніми» державами, інформаційне протиборство між провідними державами світу, зокрема у військово-політичних цілях. Ці протиправні дії спрямовані на дестабілізацію діяльності публічних органів влади та втручання у внутрішні справи держави за допомогою інформаційних технологій.

Безпека досягається передусім шляхом конфіденційності оброблюваної інформації, а також цілісності та доступності компонентів і ресурсів системи. Потрібно враховувати насамперед ефективність системи управління інформаційними ресурсами і їхній захист, яка визначатиме загальний рівень державної безпеки. Пильну увагу слід приділити тому, що одним з найважливіших аспектів є визначення та класифікація можливих загроз безпеки [14, с. 115]. Так, В. Шемчук розглядає загрози інформаційній безпеці України як визначальні чинники, що зумовлюють і породжують негативні явища, які посягають на національні інтереси в інформаційній сфері, організацію та функціонування національного інформаційного простору загалом. Вони мають або можуть мати широкомасштабне значення, пов'язане з ризиками й небезпеками в інших сферах. При цьому, безпосередньо обумовлюють посягання на інформаційну безпеку, державний суверенітет і територіальну цілісність держави України такі загрози, як: претензії з боку інших держав світу, глобалізація світових відносин і зосередження важелів впливу на світові процеси в руках окремих осіб або груп, прояв сепаратизму й намагання автономізації за етнічною ознакою окремих регіонів України. Вони підривають фундаментальні цінності держави та суспільства, а також міжнародного правового порядку [15].

Зазначимо, що формування системи інформаційної безпеки з урахуванням національних інтересів України, запобігання (врегулювання) міждержавним конфліктам у глобальному інформаційному просторі можливе тільки на основі відповідного міжнародно-правового режиму, сприяння встановленню якого визначено головною метою державної політики в галузі міжнародної інформаційної безпеки [16]. Невід'ємною частиною цього режиму мають стати правила поведінки держав в інформаційному просторі та в умовах війни в Україні. Крім того, важливою загрозою в інформаційній сфері, що впливає на забезпечення національної безпеки, є вплив на критично важливу інфраструктуру. Ці загрози виникають внаслідок порушення функціонування інформаційних систем.

Окреслені умови неминуче тягнуть за собою заходи щодо посилення позицій України в умовах конкурентоспроможної інформаційної боротьби як з уже наявними, так і з новими центрами сили, а також щодо подальшого вдосконалення міжнародно-правового регулювання окремих положень розвитку засобів і методів захисту інформації, використовуючи передові цифрові технології.

Сучасні виклики і загрози національній інформаційній безпеці можна поділити на внутрішні та зовнішні.

До внутрішніх загроз в інформаційній сфері зараховуємо:

1) систематичне порушення правил щодо порядку користування інформацією обмеженого доступу;

2) відсутність або неналежний рівень кваліфікації персоналу у використанні інформаційних і комп'ютерних пристроїв та іншої продукції, необхідної для забезпечення інформаційної безпеки;

3) використання зарубіжних технологій і технічних засобів в інформаційних процесах;

4) порушення правових норм щодо захисту авторських прав під час створення і впровадження секретних винаходів, створених, зокрема, за державним замовленням;

5) колізії та правові прогалини у вітчизняному законодавстві при регулюванні відносин у сфері інформаційної безпеки тощо.

До зовнішніх загроз в інформаційній сфері належать:

1) активні розвідувальні та контрнаступальні заходи іноземних органів спецслужб, зокрема РФ;

2) безперервні інформаційні акти агресії за допомогою кібератак на об'єкти інформаційних інфраструктур;

3) застосування методів і засобів інформаційної війни з боку РФ, використовуючи когнітивну зброю проти національних інтересів України;

4) використання спеціальних прийомів в інформаційному просторі, які заторкують інтереси міждержавного співробітництва в галузі забезпечення інформаційної безпеки;

5) застосування методів фільтрації цифрового контенту в інтернеті задля обмеження поширення достовірної інформації про політику держави та ініціативи, що просуваються нею (це стосується, зокрема, інформації, яка висвітлюється у фейсбуку тощо).

З огляду на наведений перелік сучасних інформаційних загроз, вважаємо слушним використання комплексу правових та організаційних заходів у сфері забезпечення інформаційної безпеки:

1) формування сприятливих умов для вдосконалення кадрового потенціалу та формування резерву фахівців у сфері інформаційних технологій та інформаційної безпеки;

2) створення вітчизняного програмного продукту із захисту інформації та виявлення загроз в інформаційній системі;

3) підвищення цифрової та інформаційно-правової культури інформаційної безпеки громадян для формування стійкості до інформаційно-психологічного впливу іноземних спецслужб та впливу деструктивної ідеології;

4) вдосконалення нормативно-правової бази щодо захисту об'єктів інтелектуальної власності та інформаційної інфраструктури;

5) створення ефективних заходів щодо захисту інформації за допомогою розвитку технічного регулювання, разом з питаннями ліцензування, стандартизації та сертифікації в цій галузі;

6) розвиток міждержавного співробітництва з державами-партнерами у сфері забезпечення інформаційної безпеки за допомогою інтеграційної взаємодії, формування загальних міжнародних норм у сфері правового забезпечення інформаційної безпеки.

Висновки. На основі проведеного дослідження можна зробити висновок, що в умовах геополітичних змін і подальшої цифровізації всіх сфер життя суспільства посилилися різноманітні виклики і загрози, а також ризики в інформаційному просторі. На сучасному етапі розвитку суспільства і держави серед найактуальніших загроз національній інформаційній безпеці, зважаючи на динамічність інформаційної сфери, можна виокремити: протиправний вплив на національні інформаційні ресурси, інформаційно-телекомунікаційні системи та інформаційну інфраструктуру, разом із критично важливими інформаційними структурами; використання засобів та методів поширення недостовірної (фейкової) інформації для дезінформації людей, застосовуючи при цьому, зокрема, методи впливу на психіку людини для дезорганізації та придушення волі; несанкціоноване втручання в національний інформаційний простір. З огляду на це, трансформація інформаційного простору в умовах геополітичних змін і загострення соціально-економічних та міжнародних протиріч визначили новий вектор розвитку правового регулювання інформаційної безпеки в Україні з огляду на міжнародні стандарти у цій сфері.

Вважаємо, що формування і розвиток національної державної політики, спрямованої на забезпечення інформаційної безпеки, сприятиме подальшому вдосконаленню захисту інформаційних технологій і систем, недопущенню вразливості даних і зниженню виникнення інформаційних загроз. Вбачається, що ці заходи дадуть змогу забезпечити захист інформаційного суверенітету України, охорону суб'єктів й об'єктів високих інформаційних технологій та інноваційної інфраструктури.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини): міжнар. док. від 04.11.1950. *База даних «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 19.11.2023).
2. Нестерович В. Забезпечення інформаційної безпеки як функція держав в умовах сучасних викликів і загроз. *Fìlosofsʿkì ta metodologìčnì problemi prava*. 2020. № 1 (19). С. 136–137.
3. Гаврильців М. Т. Інформаційна безпека держави в системі національної безпеки України. *Юридичний науковий журнал*. 2020. № 2. С. 200–203.
4. «Україна – на вістрі гібридної атаки РФ у світі» – на міжнародній конференції в Академії СБУ обговорили досвід протидії інформаційним операціям РФ. *Вебсайт Національної академії Служби безпеки України.* 2021. 15 черв. URL: https://academy.ssu.gov.ua/ua/news-1-8-136-ukraina-––na-vistri-gibridnoi-ataki-rf-u-sviti-––na-mizhnarodniy-konferencii-v-akademii-sbu-obgovorili-d (дата звернення: 19.11.2023).
5. Gesetz zur Bekämpfung des internationalen Terrorismus. *Dejure.org*. URL: https://

dejure.org/BGBl/2002/BGBl._I_S._361 (viewed on 19.11.2023).
6. Legge 15 dicembre 2001, № 438 «Conversione in legge, con modificazioni, del decreto-legge 18 ottobre 2001, n. 374, recante disposizioni urgenti per contrastare il terrorismo internazionale». *Camera dei depulati*. URL: http://www.camera.it/parlam/leggi/01438l.htm#decreto (viewed on 19.11.2023).
7. Anti-terrorism, Crime and Security Act, 2001. *Legislation.gov.uk*. URL: http://www.legislation.gov.uk/ukpga/2001/24 (viewed on 19.11.2023).
8. Сек'юритизація (політологія). *Вільна енциклопедія «Вікіпедія»*. URL: https://uk.wikipedia.org/wiki/Сек%27юритизація_(політологія) (дата звернення: 19.11.2023).
9. Speech by Nicholas Howen, ICJ Secretary-General at the Biennial Conference 2004: Counter-terrorism and human rights, challenges and responses / International Commission of Jurists. URL: https://www.icj.org/wp-content/uploads/2012/04/icj_howen_biennial_speech_2004.pdf (viewed on 19.11.2023).
10. Szurlej C. Protecting Human Rights while Countering Terrorism Protecting Human Rights while Countering Terrorism a Decade after 9/11. *Researchergate*. URL: https://www.researchgate.net/publication/312279248_Protecting_Human_Rights_while_Countering_Terrorism_a_Decade_after_911 (viewed on 19.11.2023).
11. Specific Human Rights Issues: New priorities, in Particular Terrorism, 8 August 2003 / Office of UN High Commissioner for Human Rights. URL: https://www2.ohchr.org/english/issues/terrorism/docs/wp1.pdf (viewed on 19.11.2023).
12. Krasno J. E. The United Nations: Confronting the Challenges of a Global Society. Boulder, USA: Lynne Rienner Publ. 2004. 443 p.
13. 13. Золотар О.О. Правові основи інформаційної безпеки людини: автореф. дис. … д-ра юрид. наук: 12.00.07. Харків, 2018. 37 с.
14. Леоненко Н.А., Поступна О.В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник Національного університету цивільного захисту України. Сер.: Державне управління*. 2022. Вип. 2 (17). URL: http://repositsc.nuczu.edu.ua/handle/123456789/16883 (дата звернення: 19.11.2023).
15. Шемчук В.В. Забезпечення інформаційної безпеки як функція сучасних держав: порівняльно-правовий аналіз: монографія. Київ: Ліра-К, 2020. 352 с.
16. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ : Вид. дім «АртЕк», 2018. 411 с.