Інформаційне право

УДК 342.78

Бровдій Алла Михайлівна
кандидат юридичних наук, доцент,
доцент кафедри правового забезпечення господарської діяльності
Харківський національний університет
міського господарства імені О.М. Бекетова
Brovdii Alla
Candidate of Law Sciences, Docent,
Docent of the Department of Legal Support of Economic Activity
O.M. Beketov National University of Urban Economy in Kharkiv

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ОСНОВА РЕАЛІЗАЦІЇ КОНСТИТУЦІЙНИХ ПРАВ В УМОВАХ ВІЙНИ
INFORMATION SECURITY AS THE BASIS FOR THE REALIZATION OF CONSTITUTIONAL RIGHTS IN WAR CONDITIONS

Анотація. *У статті доведено, що забезпечення безпеки в інформаційному просторі є важливою функцією держави, що в умовах сьогодення має пріоритетне значення. Розглянуто поняття «інформаційна безпека», визначено її складові. Проаналізовано нормативно-правові акти, які регулюють порядок забезпечення інформаційної безпеки, а також точки зору вчених, які працювали в межах цієї тематики. Визначено, що створити дієві механізми забезпечення інформаційної безпеки можливо, в першу чергу, з урахуванням видів інформації та відповідних видів інформаційних загроз, що в умовах воєнного стану носять ще більш негативні наслідки. Реалізація громадянами передбачених Конституцією України прав в умовах воєнного стану є обмеженою з огляду на різні обставини. В першу*

чергу, такі обмеження є значними на тимчасово окупованих територіях, де обмежені права не тільки на доступ до достовірної інформації, але й інші права, передбачені Основним законом держави. Такими правами в першу чергу є право на освіту, яке наразі реалізується за допомогою інформаційно-комунікаційних технологій, доступ до яких значно обмежений у зв'язку з відсутністю стабільного доступу до мережі Інтернет, відсутністю електропостачання, обмеженням доступу до засобів зв'язку, особливо на тимчасово окупованих територіях. При цьому, їх відновлення є неможливим до моменту деокупації таких територій. Зроблено висновок про те, що розширення повноважень органів місцевого самоврядування на відповідних територіях надасть можливість ефективніше протидіяти інформаційним загрозам та дозволить оперативніше реагувати на зміну таких загроз.

Ключові слова: *інформація, інформаційна безпека, інформаційні загрози, воєнний стан, обмеження конституційних прав.*

Summary. *It is proved that ensuring security in the information space is an important function of the state, which is of paramount importance in the present conditions. The concept of "information security" is considered, its components are defined. The normative legal acts regulating the procedure for ensuring information security, as well as the points of view of scientists who worked within this topic are analyzed. It is determined that the possibility of the creation of effective mechanisms for ensuring information security, first of all, are possible taking into account the types of information and the corresponding types of information threats, which under martial law have even more negative consequences. The exercise by citizens of the rights provided for by the Constitution of Ukraine under martial law is limited due to various circumstances. First of all, such restrictions are significant in the temporarily occupied territories, where the rights not only to access reliable information are*

limited, but also other rights provided for by the Basic Law of the state. Such rights are primarily the right to education, which is currently being implemented through information and communication technologies, access to which is significantly limited due to the lack of stable access to the Internet, the lack of electricity supply, and the restriction of access to communications, especially in the temporarily occupied territories. At the same time, their restoration is impossible until the de-occupation of such territories. It is concluded that the expansion of the powers of local self-government bodies in the relevant territories will provide an opportunity to more effectively counteract information threats and will allow to respond more quickly to changes in such threats.

Key words: *information, information security, information threats, military status, restriction of constitutional rights.*

Постановка проблеми. Розвиток українського суспільства сьогодні відбувається в умовах не тільки збройної агресії, але й у інформаційному просторі. Інформація в сучасному суспільстві є основою розвитку усіх сфер діяльності людини: бізнесу, освіти, науки, культури, соціального забезпечення, праці, охорони здоров'я, інноваційної діяльності, реалізації особистих прав людини тощо. Вона є основою прийняття управлінських рішень як в державі так і на рівні органів місцевого самоврядування, суб'єктів господарювання, окремих осіб. Отримання, використання та розповсюдження інформації забезпечує можливість бути учасником різних суспільних відносин, що є необхідним та важливим аспектом існування держави. У в'язку зі вказаним, забезпечення безпеки інформації, особливо інформації, що міститься в електронних базах даних, є пріоритетним напрямом державної інформаційної політики, що прямо передбачено в Законі України «Про інформацію» [11], і є основою розвитку інших сфер діяльності держави. Так, відповідно до положень Закону України «Про

Концепцію Національної програми інформатизації», вона є невід'ємною частиною політичної, економічної, оборонної та інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і електронної комунікації, механізми забезпечення функціонування електронних комунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни [12]. В умовах воєнного стану зазначені об'єкти інформаційної безпеки стають більш уразливими, що вимагає як створення технічного так і правового підґрунтя для їх правового захисту. Таким чином, важливо забезпечити комплексний підхід до правового регулювання забезпечення інформаційної безпеки в умовах сьогодення, що обумовлює актуальність теми дослідження.

Аналіз останніх досліджень і публікацій. Проблеми інформаційної безпеки досліджуються вченими з різних галузей науки. Значний вклад у дослідження інформаційних правовідносин зробили такі вчені як М. Баран [2], І. Панова [9], В. Ткаченко [16], О. Рижук [15], Ю. Муравська [8], А. Шевцова [17] та інші. Ґрунтовне дослідження щодо забезпечення інформаційної безпеки здійснив О. Панченко, який сформував методологічне підґрунтя щодо забезпечення інформаційної безпеки держави як основи її функціонування, яке включає необхідність нормативно-правового регулювання щодо протидії використання інформаційних технологій, що загрожують інтересам держави, створення економічних передумов для розвитку національних інформаційних ресурсів та інфраструктури, впровадження новітніх технологій в інформаційну сферу [9]. Зміна умов, в межах яких розвивається наше громадянське суспільство потребує прийняття швидких рішень, що є важливим для забезпечення прав громадян. Вказане неможливо забезпечити без належного правового регулювання та постійного дослідження нових загроз, що виникають в суспільстві.

Формулювання цілей статті. Метою цієї статті є дослідження правових основ інформаційної безпеки та особливостей її державного забезпечення крізь призму гарантування реалізації прав громадян України в умовах воєнного стану.

Виклад основного матеріалу. Боротьба українського народу за свободу, справедливість, територіальну цілісність, а також інші права і свободи, гарантовані Конституцією України відбувається у складних соціально-економічних умовах. В умовах воєнного стану важливим є забезпечення обороноздатності держави. Проте, не менш важливим є забезпечення реалізації прав громадян, втому числі і на інформацію. Інформаційна безпека є основою для розвитку інформаційного суспільства і можливості реалізації прав і свобод громадян, визначених Конституцією України. Б. Кормич складовими сучасної системи безпеки визначає: доктрину і правову основу, якими визначаються основні завдання і принципи діяльності щодо захисту безпеки; інституціональний механізм, тобто сукупність міжнародних і національних державних і громадських органів, які у своїй діяльності вирішують певні завдання щодо підтримання стану безпеки різних рівнів; методологічну базу, тобто способи, засоби і ресурси, що використовуються для реалізації конкретних завдань у межах політики безпеки [7, с. 119]. Розглядаючи інформаційну безпеку як основу розвитку громадянського суспільства, в тому числі і в умовах воєнного стану, в першу чергу варто звернути увагу на зміст цього поняття, його нормативне та доктринальне визначення.

У абзаці 3 п. 13 Закону України «Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» [13], визначено поняття «інформаційна безпека» як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через такі дії:

1) неповноту, невчасність та невірогідність інформації, що використовується;

2) негативний інформаційний вплив;

3) негативні наслідки застосування інформаційних технологій;

4) несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Більш широке поняття інформаційної безпеки визначено в Рішенні РНБОУ від 15 жовтня 2021 року «Про стратегію інформаційної безпеки», затвердженої Указом Президента України від 28 грудня 2021 року №658/2021, відповідно до якої вона визначається як частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави. В межах інформаційної безпеки належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом. Зазначене поняття включає широке коло суспільних інтересів, в основі яких лежить інформація, що зберігається, розповсюджується та надається в різній формі і різними суб'єктами суспільних відносин. Розглядаючи це поняття можна дійти висновку, що основою забезпечення інформаційної безпеки є застосування як механізмів захисту так і превентивних механізмів для запобігання нанесення шкоди охоронюваним інтересам окремих осіб, суспільству в цілому і державі.

Відповідно до Стандарту ISO/IEC 27002 Інформаційні технології — Безпека техніки — Кодекс практики для управління інформаційною безпекою, поняття інформаційної безпеки визначається як захист інформації від широкого спектру загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику та максимізації прибутку від інвестицій і бізнес-можливостей [19]. Зазначений стандарт визначає його з точки зору забезпечення безпеки, бізнесу, тобто виходить з поняття інформаційної безпеки суб'єктів господарювання. Таким чином, визначення поняття інформаційної безпеки у зазначених нормативно-правових актах розглядається в першу чергу через поняття захищеності життєво важливих інтересів людини, суспільства, держави. Зі зміною умов, в межах яких здійснюється розвиток суспільства, змінюються пріоритетні інтереси, що потребують захисту. Як зазначає О. Золотар у монографії, виданій до введення в Україні воєнного стану, «становлення системи національної безпеки України відбувається в умовах утвердження української державності й нових суспільних відносин. Внутрішнє життя України нині характеризується болісною соціальною модернізацією, політичною невпорядкованістю, політичним і соціальним розшаруванням, яке доходить до рівня протистояння, перманентною фінансовою та економічною кризою» [6, с. 153].

Розглядаючи питання забезпечення інформаційної безпеки варто завернути увагу на види об'єктів інформаційної безпеки. З точки зору О. Довгань та Т. Ткачук, основними об'єктами інформаційної безпеки є пов'язані з національними інтересами інформація, інформаційна інфраструктура та правовий статус суб'єктів інформаційної сфери. [4]. Таким чином, можна зробити висновок, що складовими забезпечення інформаційної безпеки є: 1) забезпечення безпеки інформації, що подається через телекомунікаційні мережі, мережу Інтернет, друковані засоби масової інформації, соціальні мережі або будь-яким іншим

способом; 2) забезпечення безпеки мереж передачі інформації, що входять до інформаційної інфраструктури держави; 3) забезпечення безпеки особистих даних суб'єктів інформаційних правовідносин; 4) забезпечення безпеки суб'єктів, що володіють та розпоряджаються інформацією. При цьому варто звернути увагу на те, що безпеку інформації варто розглядати як забезпечення збереження її цілісності, доступності, достовірності, своєчасності, інформативності, безпечності.

Здебільшого інформаційна безпека визначається з точки зору забезпечення захисту інформації у мережі Інтернет, або будь-якої іншої інформації, що міститься в електронній формі. Сьогодні кібербезпека вийшла на перший план у зв'язку з тим, що більшість інформації сьогодні знаходиться у кіберпросторі, що зумовлює вищий рівень необхідності її захисту. Сьогодні в кіберпросторі ми тримаємо майже усю інформацію: домашню адресу, податкові дані, фінанси, особисту інформацію.

Не зважаючи на те, що захист електронної інформації є важливим у зв'язку з активним розвитком інформаційно-комунікаційних технологій та переведенням значної частини інформації у електронну форму, значної цифровізації України, все ж важливим також залишається забезпечення безпеки інформації, що розповсюджується за допомогою інших джерел, зокрема друкованих засобів масової інформації, фільмів, телепередач тощо. Крім цього важливого значення також набуває соціальна складова забезпечення інформаційної безпеки, що пов'язана із підвищенням рівня компетентності у сфері інформаційної безпеки та реалізації інших прав, гарантованих конституцією України. Як вказують О. Довгань та Т. Ткачук, гуманітарна складова інформаційної безпеки містить у собі величезну сукупність проблем, пов'язаних з дотриманням конституційних прав і свобод громадян у сфері духовного розвитку й інформаційної діяльності. То ж безпека інформаційної сфери не може сприйматися суто як захист телекомунікаційних мереж або мереж зв'язку, засобів масової інформації

від проникнення небажаної або шкідливої інформації [5, с. 95]. Саме принцип дотримання прав і свобод громадян повинен лежати в основі забезпечення інформаційної безпеки в різних сферах життєдіяльності суспільства і держави. Особливого значення такий принцип відіграє сьогодні з огляду на тотальні порушення прав наших громадян, суб'єктів господарювання, що здійснюють свою діяльність в межах інформаційного простору, суспільства і держави в цілому. Збройна агресія росії сьогодні супроводжується також і інформаційною війною, що порушує не тільки право на володіння, розпорядження та поширення інформації, яка є достовірною, повною, об'єктивною, доступу до неї (зокрема обмежена можливість доступу зумовлена пошкодженням об'єктів електропостачання, що унеможливлює забезпечення безперебійного зв'язку, і, відповідно доступу до інформаційних джерел), але й пов'язані з інформаційними правами, зокрема право на освіту, яка сьогодні перейшла у формат обміну інформацією через електронну мережу. Крім цього, особливих порушень щодо інформаційної безпеки також зазнають мешканці тимчасово окупованих територій, що не мають вільного доступу до інформаційних джерел, не можуть вільно розпоряджатись отриманою інформацією, а також зазнають постійних порушень у сфері використання персональних даних, отримання достовірної та повної інформації тощо.

У зв'язку з швидкою зміною факторів в умовах воєнного стану, що впливають на можливість реалізації прав громадян на інформацію, повинні змінюватись і способи забезпечення інформаційної безпеки. Як зазначає Ю. Муравська, безпека не повинна розглядатися як незалежна змінна, оскільки вона має наступні характеристики:

– динамічна і процесуальна – підлягає постійним змінам під впливом комплексу багатофакторних явищ;

– суб'єктивна і об'єктивна – у випадку, коли соціальні відносини безпеки утворюються в результаті впливу цього явища на індивідууми, соціальні групи, суспільство;
– вирівняна, структурована;
– відносна – в залежності від кількості факторів [8].

Підтримуючи таку позицію вказаного автора можна зробити висновок, що забезпечити ефективну інформаційну безпеку можливо за умови об'єктивного аналізу обставин, що склались, визначення особливостей тих явищ, що загрожують порушенню прав громадян на інформацію та, відповідно є змінною характеристикою. Вона залежить від особливостей розвитку громадянського суспільства, обставин, в межах яких воно розвивається, економічних, політичних, соціальних та інших факторів, що існують у відповідному суспільстві у певних часових межах. В Україні значно змінились обставини та умови розвитку громадянського суспільства, що вимагає кардинальної зміни підходів до визначення інформаційної безпеки та особливостей її забезпечення. Війна змінила пріоритети держави, суспільства і окремих громадян, а також створила нові виклики, що є підставою для зміни підходів нормативно-правового регулювання у цій сфері. На думку Ю. Муравської інформаційна безпека – це стан, вільний від загроз, які сприймаються в основному як: надання інформації стороннім особам; шпигунство; саботаж та диверсійні заходи [8].

Отже, «інформаційна безпека» характеризує стан суспільства, в якому забезпечується реалізація комплексу заходів, спрямованих на попередження та подолання порушень прав громадян, пов'язаних із несанкціонованим інформаційним впливом, обмеженням доступу до інформації, можливістю її використання і розповсюдження, належне забезпечення інтересів суспільства, держави і окремих громадян в сфері інформації в умовах трансформаційних змін, що забезпечує підґрунтя для

розвитку громадянського суспільства, формування навичок критичного сприйняття інформації та забезпечення безпеки суспільства, держави та окремих суб'єктів інформаційних відносин.

Досліджуючи забезпечення інформаційної безпеки, О. Баранов наголошує на необхідності забезпечення інформаційної безпеки у трьох її складових: забезпечення запобігання завдання шкоди через неповноту, невчасність та невірогідність інформації; забезпечення запобігання нанесення шкоди через негативний інформаційний вплив; забезпечення запобігання завданню шкоди через негативні наслідки функціонування інформаційних технологій [3, с. 33].

Для забезпечення стану інформаційної безпеки в першу чергу варто визначити основні загрози, які існують у суспільстві, що становлять небезпеку для збереження інформації, її безпечного розповсюдження та подальшого використання. О. Архипов та Є. Архипова звертають увагу на те, що для побудови ефективної системи інформаційної безпеки необхідно виміряти рівень значущості (важливості, суттєвості) загроз інформації. При цьому слід враховувати, що хоч загрози можуть бути спрямовані на різні властивості інформації (конфіденційність, цілісність, доступність, надійність тощо), необхідно якимсь чином забезпечити можливість співставлення та порівняння значущості цих загроз, а також обрахування інтегральної оцінки рівня значущості всієї множини загроз [1]. Основні загрози визначені у таких нормативно-правових актах, як «Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року, затвердженої Указом Президента України від 26 серпня 2021 року №447/2021 «Про стратегію кібербезпеки України» (далі – Стратегія кібербезпеки), «Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про стратегію інформаційної безпеки», затвердженої Указом Президента України від 28 грудня 2021 року №658/2021 (далі – Стратегія інформаційної безпеки). Ці нормативно-

правові акти є основою формування державної політики у сфері інформаційної безпеки та її важливої складової кібербезпеки, яка основним пріоритетом держави, з огляду на глобальну інформатизацію майже усіх сфер діяльності суспільства і держави, оскільки саме кіберпростір, відповідно до Стратегії кібербезпеки визнано одним із можливих театрів воєнних дій [14]. Спеціальним нормативно-правовим актом у сфері забезпечення інформаційної безпеки в умовах воєнного стану є рішення Ради національної безпеки і оборони України від 18 березня 2022 року «Щодо реалізації єдиної інформаційної політики в умовах воєнного стану», введеної в дію Указом Президента України від 19 березня 2022 року №152/2022 [18]. Відповідно до цього нормативно-правового акту визначено, що в умовах воєнного стану реалізація єдиної інформаційної політики є пріоритетним питанням національної безпеки, забезпечення якої реалізується шляхом об'єднання усіх загальнонаціональних телеканалів, програмне наповнення яких складається переважно з інформаційних та/або інформаційно-аналітичних передач на єдиній інформаційній платформі стратегічної комунікації.

Відповідно до Стратегії інформаційної безпеки, інформаційна загроза визначена як потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

З метою більш ефективного забезпечення інформаційної безпеки варто також розподілити інформацію на види, що створить передумови для запровадження дієвих механізмів у цій сфері.

Так, залежно від сфери розповсюдження інформації, можна виділити такі її види: 1) технологічна інформація, 2) критична технологічна

інформація; 3) конфіденційна інформація; 4) персональні дані; 5) таємна інформація; 6) службова інформація; 7) інформація про особу; 8) інформація про діяльність суб'єкта господарювання; 9) освітня інформація; 10) публічна інформація; 11) інформація, що є державною таємницею.

Залежно від способу отримання та розповсюдження інформації: 1) електронна; 2) друкована; 3) усна; 4) отримана за допомогою телекомунікаційних мереж; 5) отримана із соціальних мереж.

Щодо кожного з видів інформації можна виділити окремі види інформаційних загроз, проте наразі основною загрозою інформаційної безпеки, України, що торкається усіх видів інформації є війна, розпочата росією на території нашої держави, яка створює нові виклики і загрози для розвитку нашого громадянського суспільства, порушує усі передбачені Конституцією України права громадян, в тому числі і права на інформацію, а також похідні від неї права. Вона значно впливає на можливість реалізації конституційних прав і свобод громадян, що вимагає від держави змін правового забезпечення інформаційної безпеки та прийняття нових нормативно-правових актів у цій сфері, а також забезпечення оперативного реагування на нові загрози інформаційній безпеці, що може бути реалізовано шляхом надання більш широких повноважень органам місцевого самоврядування, а також органам державної влади на місцях (військовим адміністраціям). Наразі, відповідно до Закону України «Про правовий режим воєнного стану», одним із заходів правового режиму воєнного стану, що запроваджується військовим командуванням разом із військовими адміністраціями є регулювання у порядку, визначеному Кабінетом Міністрів України, роботи постачальників електронних комунікаційних мереж та/або послуг, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій і закладів культури та засобів масової інформації, а також використання місцевих

радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз'яснювальної роботи серед військ і населення; заборона роботи приймально-передавальних радіостанцій особистого і колективного користування та передача інформації через комп'ютерні мережі. Такі повноваження є важливими, але не вирішують усіх нагальних проблем, що виникають у межах воєнного стану. Розширення повноважень місцевих органів влади у сфері забезпечення інформаційної безпеки може стати дієвим способом реалізації інформаційних прав громадян, та інших прав, що з ними пов'язані.

Висновки і перспективи подальших розвідок. Інформаційну безпеку варто розглядати як комплексне поняття, крізь призму реалізації як інформаційних прав і свобод громадян, так і похідних від них прав, реалізація яких унеможливлюється у зв'язку з порушенням прав на інформацію. Забезпечення інформаційної безпеки в умовах воєнного стану є основним пріоритетом держави, що зумовлює необхідність зміни підходів правового регулювання діяльності у цій сфері. Важливо визначити основні інформаційні загрози, що існують у суспільстві в умовах війни з урахуванням швидких трансформаційних процесів та необхідністю швидкого реагування на загрози, що виникають у ньому. Важливо розробити дієві механізми для забезпечення інформаційної безпеки, зокрема розширити повноваження місцевих органів влади у цій сфері, що створить передумови для оперативного реагування на швидку трансформацію інформаційних загроз.

До перспективних напрямів дослідження у цій сфері належать питання внесення змін до чинного законодавства України для подолання інформаційних загроз та визначення повноважень відповідних органів державної влади і місцевого самоврядування для їх належного реагування на них.

Література

1. Архипов О., Архипова Є. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» // Информационные технологии и безопасность: основы обеспечения информационной безопасности (ИТБ-2014): Материалы XIV международной научнопрактической конференции. К. : ИПРИ НАН Украины, 2014. С. 18-30. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf (дата звернення: 09.01.2023)
2. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні : дис. доктора філософії за спеціальністю 081 «Право». Львів, 2022. 242 с.
3. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки : матеріали наук.-практ. конф. ["Запобігання новим викликам та загрозам інформаційній безпеці України : правові аспекти"], (м. Київ, 6 жовт. 2016 р.) ; упоряд. : В.М. Фурашев. К : Вид-во "Політехніка", 2016. С. 29-35.
4. Довгань О.Д., Ткачук Т.Ю. Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс // Інформація і право. 2018. №2(25). С. 73-85. URL: http://ippi.org.ua/sites/default/files/9_8.pdf (дата звернення: 09.01.2023)
5. Довгань О.Д., Ткачук Т.Ю. Системи інформаційної безпеки України: онтологічні виміри // Інформація і право. 2018. № 1(24). С. 89-103.
6. Золотар О. Інформаційна безпека людини: теорія і практика : монографія. Київ : ТОВ «Видавничий дім «АртЕк», 2018. 446 с. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf (дата звернення: 09.01.2023)
7. Кормич Б.А. Інформаційне право: Підр. Х.: БУРУН і К., 2011. 334 с.
8. Муравська Ю.Є. Інформаційна безпека суспільства: концептуальний аналіз. URL:

http://dspace.wunu.edu.ua/bitstream/316497/19378/1/Муравська%28Якубівська%29_Стаття.pdf (дата звернення: 09.01.2023)

9. Панова І.В. Захист від впливу інформації,що є шкідливою для особи, як принцип інформаційного права // Право і безпека. 2010. № 3(35). С. 69-72.
10. Панченко О. А. Державне управління інформаційною безпекою в умовах турбулентності : дис. докт. держ. упр. : 25.00.05. Київ, 2020. 521 с. URL: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf (дата звернення: 09.01.2023)
11. Про інформацію : Закон України від 02.10.1992 №2657-XII // Відомості Верховної Ради України. 1992. №48. Ст. 650.
12. Про концепцію національної програми інформатизації : Закон України від 04 лютого 1998 року №75/98-ВР // Відомості Верховної Ради України. 1998. №27-28. Ст. 182 URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (дата звернення: 09.01.2023)
13. Про основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки : Закон України від 09.01.2007 №537-V // Відомості Верховної Ради України. 2007. №12. Ст. 102.
14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26 серпня 2021 року №447/2021.
15. Рижук О. Аналіз концепцій визначення «Інформаційної безпеки» в умовах глобалізації // Український науковий журнал «Освіта Регіону». Політологія психологія комунікації. 2016. №4. URL: https://social-science.uu.edu.ua/article/1400 (дата звернення: 09.01.2023)
16. Ткаченко В.А. Захист інформаційних ресурсів Сектору безпеки і оборони держави як фактор забезпечення інформаційної безпеки України / В. А. Ткаченко, П. Д. Рогов, Л. В. Бухало // Збірник

наукових праць центру воєнно-стратегічних досліджень Національного університету оборони України. 2013. № 2. С. 69-75.

17. Шевцова А.С., Панова І.В. Національна поліція України як суб'єкт формування і реалізації політики інформаційної безпеки України // Проблеми сучасної поліцеїстики : тези доп. наук.-практ. конф. (м. Харків, 20 квіт. 2022 р.). Харків, 2022. С. 281-283
18. Щодо реалізації єдиної інформаційної політики в умовах воєнного стану : рішення Ради національної безпеки і оборони України від 18 березня 2022 року введене в дію Указом Президента України від 19 березня 2022 року №152/2022.
19. ISO/IEC 27002 Інформаційні технології — Безпека техніки — Кодекс практики для управління інформаційною безпекою. URL: https://www.pdfdrive.com/bs-isoiec-270022005-bs-7799-12005bs-isoiec-177992005-information-technology-security-techniques-code-of-practice-for-information-security-management-e164647386.html (дата звернення: 09.01.2023)

References

1. Arkhypov O., Arkhypova Ye. Osoblyvosti rozuminnia poniat «informatsiina bezpeka» ta «bezpeka informatsii» // Informatsionnye tekhnologii i bezopasnost: osnovy obespecheniya informatsionnoy bezopasnosti (ITB-2014): Materialy KhIV mezhdunarodnoy nauchnoprakticheskoy konferentsii. K. : IPRI NAN Ukrainy, 2014. S. 18-30. URL: https://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf (date of access: 09.01.2023)
2. Baran M. V. Administratyvno-pravove zabezpechennia informatsiinoi bezpeky v Ukraini : dys. doktora filosofii za spetsialnistiu 081 «Pravo». Lviv, 2022. 242 s.

3. Baranov O.A. Bazovyi pryntsyp informatsiinoho prava – zabezpechennia informatsiinoi bezpeky : materialy nauk.-prakt. konf. ["Zapobihannia novym vyklykam ta zahrozam informatsiinii bezpetsi Ukrainy : pravovi aspekty"], (m. Kyiv, 6 zhovt. 2016 r.) ; uporiad. : V.M. Furashev. K : Vyd-vo "Politekhnika", 2016. S. 29-35.
4. Dovhan O.D., Tkachuk T.Iu. Pravove zabezpechennia informatsiinoi bezpeky derzhavy yak pidhaluz informatsiinoho prava: teoretychnyi dyskurs // Informatsiia i pravo. 2018. №2(25). S. 73-85. URL: http://ippi.org.ua/sites/default/files/9_8.pdf (date of access: 09.01.2023)
5. Dovhan O.D., Tkachuk T.Iu. Systemy informatsiinoi bezpeky Ukrainy: ontolohichni vymiry // Informatsiia i pravo. 2018. № 1(24). S. 89-103.
6. Zolotar O. Informatsiina bezpeka liudyny: teoriia i praktyka : monohrafiia. Kyiv : TOV «Vydavnychyi dim «ArtEk», 2018. 446 s. URL: http://ippi.org.ua/sites/default/files/informaciyna_bezpeka_lyudini_print.pdf (date of access: 09.01.2023)
7. Kormych B.A. Informatsiine pravo: Pidr. Kh.: BURUN i K., 2011. 334 s.
8. Muravska Yu.Ie. Informatsiina bezpeka suspilstva: kontseptualnyi analiz. URL:http://dspace.wunu.edu.ua/bitstream/316497/19378/1/Muravska%28Iakubivska%29_Stattia.pdf (date of access: 09.01.2023)
9. Panova I.V. Zakhyst vid vplyvu informatsii,shcho ye shkidlyvoiu dlia osoby, yak pryntsyp informatsiinoho prava // Pravo i bezpeka. 2010. № 3(35). S. 69-72.
10. Panchenko O. A. Derzhavne upravlinnia informatsiinoiu bezpekoiu v umovakh turbulentnosti : dys. dokt. derzh. upr. : 25.00.05. Kyiv, 2020. 521 s. URL: https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf (date of access: 09.01.2023)
11. Pro informatsiiu : Zakon Ukrainy vid 02.10.1992 №2657-KhII // Vidomosti Verkhovnoi Rady Ukrainy. 1992. №48. St. 650.

12. Pro kontseptsiiu natsionalnoi prohramy informatyzatsii : Zakon Ukrainy vid 04 liutoho 1998 roku №75/98-VR // Vidomosti Verkhovnoi Rady Ukrainy. 1998. №27-28. St. 182 URL: https://zakon.rada.gov.ua/laws/show/75/98-%D0%B2%D1%80#Text (date of access: 09.01.2023)
13. Pro osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007-2015 roky : Zakon Ukrainy vid 09.01.2007 №537-V // Vidomosti Verkhovnoi Rady Ukrainy. 2007. №12. St. 102.
14. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" : Ukaz Prezydenta Ukrainy vid 26 serpnia 2021 roku №447/2021.
15. Ryzhuk O. Analiz kontseptsii vyznachennia «Informatsiinoi bezpeky» v umovakh hlobalizatsii // Ukrainskyi naukovyi zhurnal «Osvita Rehionu». Politolohiia psykholohiia komunikatsii. 2016. №4. URL: https://social-science.uu.edu.ua/article/1400 (date of access: 09.01.2023)
16. Tkachenko V.A. Zakhyst informatsiinykh resursiv Sektoru bezpeky i oborony derzhavy yak faktor zabezpechennia informatsiinoi bezpeky Ukrainy / V. A. Tkachenko, P. D. Rohov, L. V. Bukhalo // Zbirnyk naukovykh prats tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy. 2013. № 2. S. 69-75.
17. Shevtsova A.S., Panova I.V. Natsionalna politsiia Ukrainy yak subiekt formuvannia i realizatsii polityky informatsiinoi bezpeky Ukrainy // Problemy suchasnoi politseistyky : tezy dop. nauk.-prakt. konf. (m. Kharkiv, 20 kvit. 2022 r.). Kharkiv, 2022. S. 281-283
18. Shchodo realizatsii yedynoi informatsiinoi polityky v umovakh voiennoho stanu : rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 bereznia 2022 roku vvedene v diiu Ukazom Prezydenta Ukrainy vid 19 bereznia 2022 roku №152/2022.

19. ISO/IEC 27002 Informatsiini tekhnolohii — Bezpeka tekhniky — Kodeks praktyky dlia upravlinnia informatsiinoiu bezpekoiu. URL: https://www.pdfdrive.com/bs-isoiec-270022005-bs-7799-12005bs-isoiec-177992005-information-technology-security-techniques-code-of-practice-for-information-security-management-e164647386.html (date of access: 09.01.2023)