Соціально-правові студії. 2021. Випуск 3 (13). С. 50-56
Social & Legal Studios. 2021. Issue 3 (13). P. 50-56

UDC (УДК) 342.6:342.922(477)
JEL Classification: K 10; K 23

Баран Марія Володимирівна,
здобувач освітнього ступеня доктора філософії у галузі права
кафедри адміністративно-правових дисциплін
Львівського державного університету внутрішніх справ
(Львів, Україна)
e-mail: baranmaria17@ukr.net
ORCID ID: 0000-0002-2434-855X

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК ПРЕДМЕТ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ

Анотація. Розглянуто інформаційну безпеку як предмет адміністративно-правового регулювання. Базовим методом дослідження застосовано комплексний системний підхід, на підставі якого проведено загальне та структурне дослідження питань інформаційної безпеки, з якими стикаються особа, суспільство і держава. Багатосуб'єктність у галузі інформації та безпеки визначає складність, важливість та актуальність дослідження проблеми з погляду науки адміністративного й інформаційного права. Розкрито взаємний зв'язок національної та інформаційної безпеки, джерела загроз інформаційній безпеці й способи протидії. Встановлено, що як предмет діяльності, спрямованої на забезпечення інформаційної безпеки, потрібно розглядати сукупність упорядкованих правовим забезпеченням суспільних відносин, адміністративно-правове регулювання яких залежить від можливих зовнішніх впливів. Предметній сфері адміністративно-правового регулювання інформаційної безпеки характерні такі ознаки: невід'ємність інформаційних відносин або обумовленість ними; взаємопов'язаність і взаємозалежність інформаційних відносин з об'єктами національних інтересів в інформаційній сфері; взаємозв'язок адміністративно-правового регулювання інформаційної безпеки з урахуванням виникнення, виявлення та запобігання загрозам національним інтересам в інформаційній сфері з метою розроблення та застосування механізмів ефективної протидії загрозам. Указано, що діяльність із забезпечення інформаційної безпеки виражається в адміністративно-правовому регулюванні, предметна спрямованість якого визначається сукупністю суспільних відносин в інформаційній сфері, спрямованій на зміцнення рівноправного стратегічного партнерства у галузі інформаційної безпеки з НАТО і ЄС, захисті суверенітету України в інформаційному просторі.

Ключові поняття: інформація, інформаційна безпека, інформаційна інфраструктура, адміністративно-правове регулювання, національні інтереси.

Baran Maria,
Postgraduate Student
of the Department of Administrative Law Disciplines,
Lviv State University of Internal Affairs
(Lviv, Ukraine)
e-mail: baranmaria17@ukr.net
ORCID ID: 0000-0002-2434-855X

INFORMATION SECURITY AS A SUBJECT OF ADMINISTRATIVE AND LEGAL REGULATION

Abstract. Information security as a subject of administrative and legal regulation is considered. The basic method of the research is a comprehensive system approach, on the basis of which a general and structural study of information security issues faced by the individual, society and the state is conducted. A comprehensive systematic approach is used by the basic method of the research, on the basis of which a general and structural study of information security issues faced by the individual, society and the state. The multifaceted nature of information and security determines the complexity, importance and relevance of the research on the problem from the point of view of the science of administrative and information law. The interrelation of national and information security, sources of threats to information security and ways of counteraction are revealed. It is established that as a subject of activity aimed at ensuring information security, it is necessary to consider a set of social relations regulated by legal support, the administrative and legal regulation of which depends on possible external influences. The subject area of administrative and legal regulation of information security has the following features: the inseparability of

information relations or their conditionality; interconnectedness and interdependence of information relations with objects of national interests in the information sphere; the relationship of administrative and legal regulation of information security, taking into account the emergence, detection and prevention of threats to national interests in the information sphere in order to develop and apply mechanisms to effectively combat threats. Information security activities are expressed in administrative and legal regulation, the subject orientation of which is determined by a set of public relations in the information sphere, aimed at strengthening equal strategic partnership in the field of information security with NATO and the EU, protection of Ukraine's sovereignty in the information space.

Key concepts: information, information security, information infrastructure, administrative and legal regulation, national interests.

DOI 10.32518/2617-4162-2021-3-50-56

Вступ

Інформація безпосередньо впливає на різні характеристики, умови функціонування та розвитку всіх наявних систем, головною з яких є безпека. Безпека є однією із фундаментальних основ суспільства і держави, законодавчо цей термін не визначено. Безпека об'єкта може бути визначена як результат цілеспрямованого зовнішнього впливу, який спонукав напрацювання певного набору стандартів, дотримання яких передбачає гарантію необхідного ступеня захищеності об'єкта від реальних і потенційних загроз. Будучи самостійним об'єктом правового регулювання, інформація зумовлює межі та рівні безпеки залежно від якісних, смислових і кількісних характеристик, обліку прогнозованих і наявних загроз. Стандарти, обмеження, заходи безпеки сукупно утворюють умови, які у підсумку надають можливість існування об'єкту захисту.

Питання адміністративно-правового регулювання та забезпечення інформаційної безпеки досліджували вчені-юристи, а саме: В. Б. Авер'янов, О. А. Баранов, Л. Р. Біла, Ю. П. Битяк, К. В. Бондаренко, В. М. Брижко, В. М. Гаращук, Т. О. Гаврилюк, І. С. Грищенко, С. С. Єсімов, Д. Г. Заброда, О. О. Золотар, О. М. Музичук, В. К. Колпаков, Т. О. Коломоєць, О. В. Кузьменко, Р. А. Калюжний, М. В. Ковалів, Б. А. Кормич, С. В. Ківалов, Д. М. Лук'янець, І. Д. Пастух, С. В. Пєтков, А. І. Собакарь, Ю. С. Шемшученко, В. О. Шамрай та інші. Вдосконалення інформаційних технологій зумовлює необхідність у теоретичному і практичному осмисленні проблематики, пов'язаної з адміністративно-правовим регулюванням інформаційної безпеки, що на тлі недоліків законодавства визначає актуальність дослідження.

Метою статті є визначення сутності інформаційної безпеки як предмета адміністративно-правового регулювання.

1. Взаємний зв'язок національної та інформаційної безпеки

Національна безпека має міждисциплінарний характер, об'єднує зміст усіх відомих видів безпеки, включає не тільки оборону країни, а й передбачені законодавством України: державну, суспільну, екологічну, транспортну, енергетичну, інформаційну, економічну безпеку тощо. Всі види безпеки взаємопов'язані, доповнюють одна одну й опосередковані стосовно рівня національної безпеки.

Проблема національної безпеки, як випливає з дефініції, укладеної в Законі України «Про національну безпеку України», пов'язана із забезпеченням інформаційної безпеки, що посідає виняткове місце у системі національної безпеки, будучи ключовим аспектом. Це пов'язано з тим, що інформація може мати не так соціально корисний характер, як становити серйозну загрозу безпеці особи, суспільства та держави [1].

Поєднання офіційних поглядів на поставлені цілі, завдання, на вирішення яких спрямовані зусиль, принципи, методологія, основні напрями забезпечення інформаційної безпеки держави, є доволі переконливими і послідовно представлені у нормативно-правовому акті – Доктрині інформаційної безпеки України, прийнятій у 2017 році, згідно з якою під інформаційною безпекою розуміється стан захищеності особи, суспільства та держави від внутрішніх і зовнішніх інформаційних загроз, за якого забезпечується не тільки реалізація конституційних громадянських прав і свобод людини та громадянина, гідна якість і рівень життя громадян, а й суверенітет, територіальна цілісність і стійкий соціально-економічний розвиток України, оборона й безпека держави [2].

Проблема забезпечення безпеки посилюється зовнішніми та внутрішніми викликами, значною кількістю загроз в умовах сучасних глобальних змін, які характеризуються інтеграцією економіки України у світове господарство, до Європейського Союзу, Організації економічного співробітництва і розвитку, Північноатлантичного договору (НАТО), інших міжнародних інститутів на основі повноправного партнерства [3]. Не можна не враховувати посилення політичного й економічного тиску на Україну з боку Російської Федерації і тен-

денції, що намітилася, стосовно зміни курсу значної кількості країн щодо російської експансії до відстоювання національних інтересів.

Вивчення проблематики проведення теоретико-правових досліджень, пов'язаних із моделюванням процесів, що відбуваються у правовому механізмі правового регулювання застосування інформаційних технологій у публічному управлінні в результаті функціонування й обумовлених його характеристиками як складної синергетичної системи, дає змогу окреслити коло питань, які потребують переосмислення: процес взаємодії підсистем правового механізму, що визначає виникнення правового регулювання як сукупної, інтегративної властивості; можливі варіанти поведінкових реакцій механізму правового регулювання застосування інформаційних технологій як складної синергетичної системи [4, с. 219].

З огляду на ці позиції, доцільно структурувати правовідносини, що виникають у сфері інформаційної безпеки.

Об'єктами інформаційної безпеки є: держава, суспільство, особа, її законні інтереси, права та свободи, безпосередньо пов'язані з виробництвом, застосуванням, поширенням інформації, цінністю використовуваних інформаційних ресурсів і встановленим механізмом доступу, та безпосередньо інформація і інформаційні ресурси.

Рівень захищеності об'єкта інформаційної безпеки залежить від ступеня ефективності функціонування суб'єктів забезпечення від внутрішніх властивостей і якостей об'єкта, дослідження і обліку, які є обов'язковою умовою під час розроблення заходів, спрямованих на забезпечення інформаційної безпеки.

Інформаційна безпека розглядається поряд із кібербезпекою, захистом персональних даних, недоторканністю особистого життя і прав користувачів цифрових технологій, зміцненням та захистом довіри у кіберпросторі, визначається передумовою одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками [5, с. 100].

Суб'єкти забезпечення інформаційної безпеки є цілісною системою, що охоплює державні органи законодавчої та виконавчої влади, інші уповноважені посадові особи, об'єднання, установи, громадські організації, які здійснюють правове регулювання та відповідальні за розроблення і реалізацію необхідних заходів безпеки у межах компетенцій, якими вони володіють.

Головним суб'єктом реалізації завдань у сфері адміністративно-правового регулювання є органи виконавчої влади, які наділені адміністративно-юрисдикційними повноваженнями щодо застосування заходів адміністративно-правового впливу за правопорушення, вчинені в інформаційній сфері.

Одним із завдань, пов'язаних з правовим регулюванням інформаційної безпеки, є розмежування компетенції органів публічної влади й управління так, щоб досягти максимальної ефективності діяльності, спрямованої на протидію загрозам. Проблема взаємодії суб'єкта й об'єкта управління при виробленні цілей управління нині набуває особливої актуальності й специфіки [6, с. 12].

Компетенція органу державної влади безпосередньо залежить не тільки від повноважень, предметів відання, а й функцій, делегованих державою для провадження діяльності, що формується з урахуванням різних факторів. Рішення необхідне для досягнення стратегічно важливої мети – напрацювання правового механізму, за якого забезпечується захист прав і законних інтересів усіх суб'єктів інформаційних правовідносин.

Інтереси особи в сфері інформаційної безпеки полягають у дотриманні, реалізації задекларованих Конституцією України прав на пошук, отримання, ознайомлення, використання, поширення інформації, реалізацію конституційних і громадянських прав людини на недоторканність приватного життя при застосуванні інформаційних технологій, захист прав на об'єкти інтелектуальної власності, у забезпеченні прав і законних інтересів громадянина на захист здоров'я від неусвідомлюваної шкідливої інформації.

Інформаційні інтереси суспільства пов'язані із забезпеченням державою інформаційної підтримки різних демократичних інститутів, різноманітних механізмів взаємодії держави та громадянського суспільства, збереженням культурних, історичних і моральних цінностей народу України.

Державні інтереси в інформаційній сфері полягають у створенні необхідних умов із метою реалізації інтересів особи та суспільства в інформаційній сфері, формуванні інститутів громадського контролю органів державної влади, забезпеченні законності та правопорядку, розвитку інформаційної інфраструктури, захисті державної інформаційної системи, захисті єдиного інформаційного простору країни, участі в формуванні ефективної системи міжнародної інформаційної безпеки.

Інтереси держави доцільно поділити на чотири функціональні частини: дотримання конституційних прав і свобод людини та громадянина у сфері отримання та обігу інформації; забезпечення своєчасності, достовірності,

повноти інформації, що стосується державної політики щодо соціально значущих подій у країні та світі; розвиток галузі інформаційних і комунікаційних технологій, розроблення, виробництво, експлуатація засобів забезпечення інформаційної безпеки, надання послуг у сфері інформаційної безпеки, забезпечення функціонування інформаційної інфраструктури; участь у формуванні системи міжнародної інформаційної безпеки.

2. Джерела загроз інформаційній безпеці та способи протидії

Джерела загроз інформаційній безпеці поділяються на дві групи: зовнішні, пов'язані з діяльністю держави у сфері зовнішньої політики, внутрішні загрози, що формуються виходячи з соціально-економічного стану суспільства.

Діяльність Російської Федерації пов'язана з інформаційно-технічним впливом на інформаційну інфраструктуру України з метою досягнення економічної та військової переваги; активізацією всіх видів розвідки і насамперед технічної щодо органів державної влади, організацій, які провадять наукову діяльність; дестабілізацією внутрішньополітичної та соціальної обстановки в державі різними деструктивними силами; розв'язанням повномасштабної інформаційної війни, спрямованої на населення країни з метою переорієнтування на культурні духовно-моральні цінності «руського миру»; фактичною реалізацією терористичної та сепаратиської діяльності на території держави. Це невелика частина найнебезпечніших зовнішніх загроз в інформаційній сфері.

Одними з внутрішніх загроз забезпечення інформаційної безпеки є криміногенна обстановка, йдеться не так про зростання злочинності, як про переорієнтування її у фінансову сферу, в галузь конституційних прав і свобод, пов'язаних з інформацією, при активному застосуванні інформаційних технологій на тлі реформи державного управління, що триває доволі тривалий час; низький ступінь ефективності наукових досліджень у сфері інформаційних технологій, недостатнє кадрове забезпечення у галузі інформаційної безпеки, пов'язане з проблемами системи освіти. Це не повний перелік загроз інформаційній безпеці, на протидію яким повинні бути спрямовані зусилля органів публічної влади. Однозначно диференціювати загрози по походженню, природі, за іншими ознаками, враховуючи взаємозалежність життєвих процесів, майже неможливо.

Із погляду на режими інформаційної безпеки, де об'єктом права є інформація, а у разі інформаційного забезпечення суб'єктів інформаційних відносин, режими інформації у мережі інтернет, вибірку даних з об'єктів різних класів за заданим атрибутом зробити складно. Це зумовлено об'єднанням сфери інформаційної безпеки у різних напрямах діяльності людини з однієї позиції – інформації як правового, так і математичного явища [7, с. 18].

Спроба реалізації загроз – взаємовідношення об'єкта і суб'єкта в інформаційному процесі з протилежними інтересами, пропонується розглядати з позиції активності у дії, яка призводить до наслідків критичного характеру, що виражаються не тільки в порушенні режиму конфіденційності інформації, цілісності, доступності та достовірності, а й у функціонуванні інформаційних систем. Загрози об'єктам інформаційної інфраструктури можуть бути реалізовані різними способами подолання системи інформаційної безпеки, наприклад, інформаційними, програмними, фізичними, телекомунікаційними, організаційно-правовими.

До інформаційного способу можна віднести неправомірний доступ до інформації, що призводить до витоку; незаконне збирання, поширення, використання інформації; маніпулювання інформацією та розкрадання з баз даних; модифікацію та копіювання даних і програм із порушенням правил, незаконне знищення інформації; порушення умов інформаційного обміну.

Програмні методи порушення інформаційної безпеки – технічна процедура щодо впровадження програм-вірусів, програмних закладок на стадії проєктування, у процесі експлуатації інформаційної системи, які руйнують системи захисту інформації.

Фізичні способи порушення інформаційної безпеки характеризуються різноманітністю, зокрема: знищення, розкрадання, руйнування засобів обробки та захисту інформації, засобів комунікації; знищення, розкрадання та руйнування оригіналів носіїв інформації; розкрадання ключів засобів криптографічного захисту інформації, програмних або апаратних ключів засобів захисту інформації від несанкціонованого доступу; вплив на персонал і користувачів системи з метою створення сприятливих умов для реалізації загроз інформаційній безпеці.

До телекомунікаційних способів належать: перехоплення, дешифрування інформації, витік технічними каналами; впровадження пристроїв у засоби обробки інформації, у приміщення, де інформація циркулює; нав'язування недостовірної інформації у мережах передачі даних, електронне блокування ліній комунікацій і систем управління [8, с. 144].

Організаційно-правові способи порушення інформаційної безпеки зводяться до

невиконання вимог правових норм, що регулюють відносини у сфері інформаційної безпеки, недостатньої ефективності й оперативності роботи органів влади при прийнятті нормативно-правових актів у сфері інформаційної безпеки; недосконалості юридичних норм і практики застосування права, прийняті норми наразі мало відображаються у суспільно-політичних реаліях: відчутні недоліки загальної культури дотримання встановлених норм як політичними суб'єктами, інститутами державної влади різних рівнів, так і широкими масами громадян; повільне впровадження стандартів НАТО [9, с. 23].

Нові виклики та загрози в інформаційній сфері призвели до розуміння того, що значення такої функції держави, як правове регулювання суспільних відносин у галузі протидії загрозам національним інтересам держави в інформаційній сфері, зросла. Наявність зазначеного комплексу суспільних відносин, наділених певною специфікою, говорить про те, що досліджуване правове утворення є самостійним предметом адміністративно-правового регулювання, дає змогу виокремити три предметні галузі:

– забезпечення безпеки інформації щодо окремих інформаційних об'єктів, або інформаційних ресурсів, які входять до інформаційних баз чи інформаційних систем;

– забезпечення безпеки суб'єктів правовідносин від соціально небезпечної або шкідливої інформації, зокрема шкідливої для функціонування інформаційних і телекомунікаційних систем, інформації з обмеженим доступом;

– забезпечення безпеки прав і законних інтересів суб'єктів правовідносин у разі несанкціонованого доступу до інформації, комунікацій, програмного забезпечення.

Суспільні відносини у сфері інформаційної безпеки мають характерні ознаки. Зміст першої ознаки ґрунтується на невід'ємності інформаційних відносин або зумовленості ними. Невід'ємність і обумовленість інформаційних відносин зумовлені підставою виникнення, тобто юридичним фактом або сукупністю таких фактів.

Позначений елемент правового регулювання полягає не тільки у реалізації права у сфері інформаційної безпеки суб'єктів, які вступають у відносини, а й у результаті регулювального впливу держави як головного суб'єкта правовідносин у цій галузі, на волю учасників, на інформацію, що є ключовим об'єктом інформаційних відносин.

Суб'єкти правовідносин мають право на доступ до інформації, можливість отримати інформацію, ознайомлюватися, використовувати інформацію, змінювати склад і властивості, виходячи з наявних повноважень, обраних цілей і завдань, установлених правовими нормами. У результаті діяльності щодо забезпечення інформаційної безпеки реалізуються загальні принципи та вимоги до стану захищеності не тільки власних інтересів, а й прав, законних інтересів інших учасників правовідносин.

Така взаємозалежність діяльності суб'єктів і інформації створює умови для формування стабільності управлінських відносин в організованій і впорядкованій системі інформаційної безпеки, що є головною метою адміністративно-правового регулювання відносин у зазначеній сфері діяльності. Адміністративно-правове регулювання забезпечення інформаційної безпеки – це сукупність закріпленої в законодавстві системи заходів і прийомів, спрямованих на забезпечення безпечної діяльності в інформаційному просторі, що динамічно розвивається, фізичних і юридичних осіб, сприятливої для інновацій, інвестицій, яка забезпечує населення, високого рівня життя і економічного прогресу. Тому зміст адміністративно-правового регулювання інформаційних відносин вимагає обґрунтування у межах адміністративно-правового режиму інформаційної безпеки [10, с. 128].

Друга ознака – взаємопов'язаність і взаємозалежність інформаційних відносин з об'єктами національних інтересів в інформаційній сфері. Рівень і стан інформаційної безпеки держави як головного суб'єкта правовідносин, що здійснює адміністративно-правове регулювання інформаційних відносин повинні відповідати цілям і завданням, спрямованим на реалізацію національних інтересів у інформаційній сфері.

Відповідно до Доктрини інформаційної безпеки України, національні інтереси представляють об'єктивно значущі потреби учасників правовідносин в інформаційній сфері. Інформаційна безпека охоплює сукупність інформації і інформаційної інфраструктури, інформаційних технологій, суб'єктів правовідносин і механізмів, що здійснюють регулювання відповідних суспільних відносин.

Інформація і інформаційна інфраструктура виконують роль об'єктів інформаційної безпеки, а інформаційні технології, згідно з Законом України «Про захист інформації в інформаційно-телекомунікаційних системах», представляють процес або діяльність суб'єктів правовідносин в інформаційній сфері [11]. Інформаційна сфера – це сукупність об'єктів і суб'єктів правовідносин, діяльності суб'єктів у цій сфері, спрямованої на реалізацію прав і законних інтересів, механізмів регулювання суспільних відносин. Ця ознака відображає інтерес, який виявляють суб'єкти правовідносин до об'єктів інформаційної сфери.

Третя ознака – це взаємозв'язок адміністративно-правового регулювання інформаційної безпеки з урахуванням виникнення, виявлення та запобігання загрозам національним інтересам в інформаційній сфері з метою розроблення та застосування механізмів ефективної протидії загрозам. Розгляд дефініції «безпека» у науковій літературі призвів до висновку, що основною характеристикою є загальний стан захищеності об'єкта від впливу зовнішніх сил.

Поняття «забезпечення інформаційної безпеки» охоплює такі елементи: об'єкт інформаційної безпеки, загрози стану захищеності об'єкта, суб'єкт забезпечення інформаційної безпеки, діяльність суб'єктів інформаційної безпеки, засоби забезпечення інформаційної безпеки.

Основним критерієм, що характеризує стан захищеності об'єкта в інформаційній сфері, є порушення безпеки інформаційних ресурсів, інформаційних технологій, прав і законних інтересів суб'єктів правовідносин, яке може виявлятися у виді загроз, ризиків, правопорушень.

Найбільш небезпечним порушенням інформаційної безпеки є загроза, умисний зовнішній вплив щодо певної організації або інформаційної системи, яка передбачає завдання збитку певним властивостям або складовим об'єкта безпеки. Однією з таких загроз є порушення встановлених правил доступу до інформації (несанкціонований доступ).

Для запобігання завдання шкоди або принаймні мінімізації необхідно створити відповідні умови, сформувати систему забезпечення інформаційної безпеки. Відповідальність за створення системи покладається на суб'єктів правовідносин у сфері інформаційної безпеки, головна мета діяльності яких полягає у протидії загрозам із використанням засобів, призначених для забезпечення інформаційної безпеки. Суб'єкти й об'єкти правовідносин у сфері інформаційної безпеки можуть піддаватися загрозам. Суспільні відносини, що розглядаються, об'єктами яких є інформація та інформаційна інфраструктура, стають предметом діяльності, спрямованої на забезпечення інформаційної безпеки.

Висновки

Як предмет діяльності, спрямованої на забезпечення інформаційної безпеки, потрібно розглядати сукупність упорядкованих правовим забезпеченням суспільних відносин, адміністративно-правове регулювання яких залежить від можливих зовнішніх впливів. Предметній сфері адміністративно-правового регулювання інформаційної безпеки характерні такі ознаки: невід'ємність інформаційних відносин або обумовленість ними; взаємопов'язаність і взаємозалежність інформаційних відносин з об'єктами національних інтересів в інформаційній сфері; взаємозв'язок адміністративно-правового регулювання інформаційної безпеки з урахуванням виникнення, виявлення та запобігання загрозам національним інтересам в інформаційній сфері з метою розроблення та застосування механізмів ефективної протидії загрозам.

Діяльність із забезпечення інформаційної безпеки виражається в адміністративно-правовому регулюванні, предметна спрямованість якого визначається сукупністю суспільних відносин в інформаційній сфері, спрямованої на зміцнення рівноправного стратегічного партнерства у галузі інформаційної безпеки з Організацією північноатлантичного договору (НАТО) і Європейським Союзом, захисті суверенітету України в інформаційному просторі, протидії загрозам використання інформаційних технологій з метою порушення стабільності економічного розвитку та зміні стратегічного курсу європейської інтеграції, забезпеченні територіальної цілісності та суверенітету України. Залишається чимало проблем, для усунення яких потрібні подальші дослідження у контексті забезпечення захисту особи, суспільства та держави від зовнішніх і внутрішніх інформаційних загроз.

Список використаних джерел

1. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text
2. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» : Указ Президента України від 25.02.2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/ 2017#Text
3. Підписано оновлену редакцію Дорожньої карти Україна-НАТО з оборонно-технічного співробітництва. Урядовий портал. 13 грудня 2019 р. URL: https://www.kmu.gov.ua/news/pidpisano-onovlenu-redakciyu-dorozhnoyi-karti-ukrayina-nato-z-oboronno-tehnichnogo-spivrobitnictva
4. Єсімов С. С. Методологія дослідження інформаційних технологій у публічному управлінні. *Науковий вісник Львівського державного університету внутрішніх справ. Серія юридична.* 2017. Вип. 4. С. 211–221.
5. Бондаренко Р. В., Михальчук М. В. Інформаційна безпека держави. *Інвестиції: практика та досвід.* 2021. № 5. С. 95–101.

6. Адміністративне право України (загальна частина) : навчальний посібник / О. І. Остапенко, М. В. Ковалів, Л. С. Гулак та інші. Львів : НУ «Львівська політехніка», 2019. 504 с.
7. Малашко О. Є., Єсімов С. С. Нормативно-правове забезпечення інформаційної безпеки в Україні. *Інтернаука.* 2020. № 14 (94). Т. 2. URL: http://dspace.lvduvs.edu.ua/bitstream/1234567890/3369/1/%d1%94%d1%81%d1%96%d0%bc%d0%be%d0%b2.pdf
8. Жарков Я. М., Дзюба М. Т., Замаруєва І. В. Інформаційна безпека особистості, суспільства, держави : підручник. Київ : ВПЦ «Київський університет», 2008. 274 с.
9. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. на здобуття наук. ступеня д-ра політичних наук : 23.00.02. Львів, 2021. 37 с.
10. Перун Т. С. Адміністративно-правовий механізм забезпечення інформаційної безпеки в Україні : дис. … канд. юрид. наук : 12.00.07. Львів, 2019. 268 с.
11. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua /laws/card/80/94-%D0%B2%D1%80

References

1. Pro natsional′nu bezpeku Ukrayiny : Zakon Ukrayiny vid 21.06.2018 r. № 2469-VIII [On the national security of Ukraine: Law of Ukraine of June 21, 2018 № 2469-VIII]. Retrieved from https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukr.].
2. Pro rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 29 hrudnya 2016 roku «Pro Doktrynu informatsiynoyi bezpeky Ukrayiny» : Ukaz Prezydenta Ukrayiny vid 25.02.2017 r. № 47/2017 [On the decision of the National Security and Defense Council of Ukraine of December 29, 2016 «On the Doctrine of Information Security of Ukraine»: Decree of the President of Ukraine of 25.02.2017 № 47/2017]. Retrieved from https://zakon.rada.gov.ua/laws/show/47/ 2017#Text [in Ukr.].
3. Pidpysano onovlenu redaktsiyu Dorozhn′oyi karty Ukrayina-NATO z oboronno-tekhnichnoho spivrobitnytstva. Uryadovyy portal. 13 hrudnya 2019 r. [An updated version of the NATO-Ukraine Roadmap for Defense and Technical Cooperation has been signed. Government portal. December 13, 2019]. Retrieved from https://www.kmu.gov.ua/news/pidpisano-onovlenu-redakciyu-dorozhnoyi-karti-ukrayina-nato-z-oboronno-tehnichnogo-spivrobitnictva [in Ukr.].
4. Yesimov, S. S. (2017). Metodolohiya doslidzhennya informatsiynykh tekhnolohiy u publichnomu upravlinni [Methodology of information technology research in public administration]. *Naukovyy visnyk L'vivs'koho derzhavnoho universytetu vnutrishnikh sprav. Seriya yurydychna*, 4, 211–221 [in Ukr.].
5. Bondarenko, R. V. & Mykhal′chuk, M. V. (2021). Informatsiyna bezpeka derzhavy. Investytsiyi: praktyka ta dosvid [Information security of the state. Investments: practice and experience], 5, 95–101 [in Ukr.].
6. Ostapenko, O. I., Kovaliv, M. V., Hulak, L. S. i inshi (2019). Administratyvne pravo Ukrayiny (zahal′na chastyna) [Administrative law of Ukraine (general part)]. L′viv : NU «L′vivs′ka politekhnika» [in Ukr.].
7. Malashko, O. Ye. & Yesimov, S. S. (2020). Normatyvno-pravove zabezpechennya informatsiynoyi bezpeky v Ukrayini [Regulatory and legal support of information security in Ukraine]. *Internauka*, 14 *(94),* 2. Retrieved from http://dspace.lvduvs.edu.ua/bitstream/1234567890/3369/1/%d1%94%d1%81%d1%96%d0%bc%d0%be%d0%b2.pdf [in Ukr.].
8. Zharkov, Ya. M., Dzyuba, M. T. & Zamaruyeva, I. V. (2008). Informatsiyna bezpeka osobystosti, suspil′stva, derzhavy. Kyyiv: VPTS «Kyyivs′kyy universytet» [in Ukr.].
9. Zakharenko, K. V. (2021). Instytutsiynyy vymir informatsiynoyi bezpeky Ukrayiny: transformatsiyni vyklyky, hlobal′ni konteksty, stratehichni oriyentyry [Institutional dimension of information security of Ukraine: transformational challenges, global contexts, strategic guidelines]. L′viv [in Ukr.].
10. Perun, T. S. (2019). Administratyvno-pravovyy mekhanizm zabezpechennya informatsiynoyi bezpeky v Ukrayini [Administrative and legal mechanism for information security provision in Ukraine]. L′viv [in Ukr.].
11. Pro zakhyst informatsiyi v informatsiyno-telekomunikatsiynykh systemakh : Zakon Ukrayiny vid 05.07.1994 r. № 80/94-VR [On protection of information in information and telecommunication systems: Law of Ukraine of 05.07.1994 № 80/94-VR]. Retrieved from https://zakon.rada.gov.ua /laws/card/80/94-%D0%B2%D1%80 [in Ukr.].

Стаття: надійшла до редакції 27.07.2021
прийнята до друку 18.08.2021
The article: is received 27.07.2021
is accepted 18.08.2021