

Науково-дослідний інститут інформатики і права
Національної академії правових наук України
Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України
Відкритий міжнародний університет розвитку людини “Україна”

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(32)/2020

Зареєстрований Міністерством юстиції України
(Свідоцтво про державну реєстрацію друкованого засобу масової інформації:
Серія КВ № 20117-9917ПР від 05.07.13 р.).

Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12),
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів кандидата наук (доктора філософії - Ph.D.)
і доктора наук у галузі юридичних наук.
Друковане періодичне видання ІНФОРМАЦІЯ І ПРАВО внесене в міжнародну базу даних
періодичних видань, згідно відповідного номеру ISSN.

м. Київ

Scientific Research Institute of Informatics and Law
of the National Academy of Law Sciences of Ukraine

Vernadsky National Library of Ukraine of
National Academy of Sciences of Ukraine

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND LAW

SCIENTIFIC PROFESSIONAL JOURNAL

№ 1(32)/2020

Registered by Ministry of Justice of Ukraine
(Certificate of state registration of printed communication media:
KV Series № 20117-9917PR dated 05.07.13).

Pursuant to Order of the Ministry of Education and Science of Ukraine dated 11.07.16 № 820 (Annex 12), the journal can publish materials related to thesis works aimed on the receipt of scientific degrees of candidate of sciences (Doctor of Philosophy-Ph.D.) and Doctor of Sciences in the area of Juridical Science.

The printed journal INFORMATION AND LAW is included in the international database of journal, in accordance with relevant ISSN number.

УДК 002:340+316.4+338.46

Наукова рада журналу**Пилипчук Володимир Григорович**, доктор юридичних наук, професор, член-кореспондентНАПрН України – *голова наукової ради*;**Бєбик Валерій Михайлович**, доктор політичних наук, професор – *зас. голови наукової ради*;**Дубровіна Любов Андріївна**, доктор історичних наук, професор, член-кореспондентНАН України – *зас. голови наукової ради*;**Куйбіда Василь Степанович**, доктор наук з державного управління, професор;**Нор Василь Тимофійович**, доктор юридичних наук, професор, академік НАПрН України;**Оніщенко Олексій Семенович**, доктор філософських наук, професор, академік НАН України;**Петришин Олександр Віталійович**, доктор юридичних наук, професор, академік НАПрН України;**Покутний Сергій Іванович**, доктор фізико-математичних наук, професор;**Савінова Наталія Андріївна**, доктор юридичних наук, с.н.с.;**Скулиш Євген Деонізієвич**, доктор юридичних наук, професор;**Таланчук Петро Михайлович**, доктор технічних наук, професор;**Тихий Володимир Павлович**, доктор юридичних наук, професор, академік НАПрН України;**Фурашев Володимир Миколайович**, кандидат технічних наук, доцент, с.н.с.;**Шемшученко Юрій Сергійович**, доктор юридичних наук, професор, академік НАН України.**Редакційна колегія****Довгань Олександр Дмитрович**, доктор юридичних наук, професор,– *голова редакційної колегії*;**Брижко Валерій Михайлович**, доктор філософії з юридичних наук, с.н.с.– *зас. голови редакційної колегії*;**Томаш Шеффлер**, доктор філософії з юридичних наук (Вроцлавський університет, Польща);**Вальдемар Беднарук**, доктор габілітований (Люблінський католицький університет, Польща);**Арістова Ірина Василівна**, доктор юридичних наук, професор;**Баранов Олександр Андрійович**, доктор юридичних наук, с.н.с.;**Бєляков Костянтин Іванович**, доктор юридичних наук, професор;**Дзьобань Олександр Петрович**, доктор філософських наук, професор;**Доронін Іван Михайлович**, кандидат юридичних наук, доцент;**Золотар Ольга Олексіївна**, доктор юридичних наук, с.н.с.;**Копан Олексій Володимирович**, доктор юридичних наук, професор;**Корж Ігор Федорович**, доктор юридичних наук, с.н.с.;**Ланде Дмитро Володимирович**, доктор технічних наук, професор;**Марущак Анатолій Іванович**, доктор юридичних наук, професор;**Настюк Василь Якович**, доктор юридичних наук, професор, член-кореспондент НАПрН України;**Ткачук Тарас Юрійович**, доктор юридичних наук, доцент.

* * * * *

UDC 002:340+316.4+338.46

THE SCIENTIFIC COUNCIL OF THE JOURNAL

Pylypchuk Volodymyr, Doctor of Juridical Science, Professor, Corresponding Member NALS of Ukraine – *Chairman of Editorial Board*;
Dubrovina Lyubov, Doctor of Historical Sciences, Professor, Corresponding Member National Academy of Sciences of Ukraine – *Vice-chairman of Editorial Board*;
Bebyk Valerii, Doctor of Political Sciences, Professor – *Vice-chairman of Editorial Board*;
Kuibida Vasyl, Doctor of Administration Science, Professor;
Nor Vasyl, Doctor of Juridical Science, Professor, Academician NALS of Ukraine;
Onishchenko Oleksii, Doctor of Philosophical Science, Professor; Academician NAN of Ukraine;
Petryshin Oleksandr, Doctor of Juridical Science, Professor, Academician NALS of Ukraine;
Pokutnyi Serhii, Doctor of Physics and Mathematics Sciences, Professor;
Savinova Nataliia, Doctor of Juridical Science, Senior researcher fellow;
Skulysh Ievhen, Doctor of Juridical Science, Professor;
Talanchuk Petro, Doctor of Engineering Sciences, Professor;
Tykhyy Volodymyr, Doctor of Juridical Science, Professor, Academician NALS of Ukraine;
Furashev Volodymyr, Candidate of Engineering Sciences, Associate Professor, Senior researcher fellow;
Shemshuchenko Yurii, Doctor of Juridical Science, Professor, Academician NAN of Ukraine.

EDITORIAL BOARD

Dovgan Oleksandr, Doctor of Juridical Science, Professor
– *Editor in Chief*
Bryzhko Valerii, Doctor of Philosophy of Juridical Science, Senior researcher fellow
– *Vice-Editor*;
Tomasz Schaffler, Doctor of Philosophy of Juridical Science (University of Wroclaw, Poland);
Waldemar Bednaruk, Doctor habilitowany (Catholic University of Lublin, Poland);
Aristova Iryna, Doctor of Juridical Science, Professor;
Baranov Oleksandr, Doctor of Juridical Science, Senior researcher fellow;
Bieliakov Konstantyn, Doctor of Juridical Science, Professor;
Dz'oban Oleksandr, Doctor of Philosophical Science, Professor;
Doronin Ivan, Candidate of Juridical Science, Associate Professor;
Zolotar Olga, Doctor of Juridical Science, Senior researcher fellow;
Kopan Oleksii, Doctor of Juridical Science, Professor;
Korzh Ihor, Doctor of Juridical Science, Senior researcher fellow;
Lande Dmytro, Doctor of Engineering Sciences, Professor;
Marushchak Anatolii, Doctor of Juridical Science, Professor;
Nastiuk Vasyl, Doctor of Juridical Science, Professor, Corresponding Member NALS of Ukraine;
Tkachuk Taras, Doctor of Juridical Science, Associate Professor.

* * * * *

З М І С Т

Інформаційне право

ДЗЬОБАНЬ О.П., РУБАН О.О. Свобода й відповідальність як аксіологічні маркери трансформації інформаційного суспільства.....	9
РАДУТНИЙ О.Е. Напрямок часу в системі права.....	22
БРИЖКО В.М., ПИЛИПЧУК В.Г. Приватність, конфіденційність та безпека персональних даних.....	33

Правова інформатика

ВАРАВА І. Інновації у професійній діяльності юристів: використання потужностей штучного інтелекту.....	47
--	----

Інформаційна і національна безпека

КОРЖ І.Ф. Концептуальні засади правової безпеки.....	55
ДОРОНІН І.М. Безпекова сутність функцій держави.....	66
СОЛОДКА О.М. Забезпечення інформаційного суверенітету держави: правовий дискурс.....	80
ГУЦАЛЮК М.В. Загрозливі тенденції організованої кіберзлочинності.....	88
ПЕТРОВ С.Г. Організаційні і правові основи вирішення проблем протидії кіберпосяганням у Європейському Союзі.....	99
ДОРОГИХ С.О. Залучення громадян до законотворчого процесу: деякі підсумки...	106
БАТИРГАРЕЄВА В.С. Концептуальна модель захисту інформаційного простору України засобами кримінального права.....	110

Інформація за іншими предметними напрямками досліджень за спеціалізаціями в галузі знань 08 – “Право”

ЖОРНЯК А.В. Про підходи до класифікації інформаційних послуг у сфері господарювання.....	120
ГОЛОВКО О.М., ДРУЗЬ В.Д. Право на правосуддя та право на доступ до інформації: кореляція та взаємозалежність.....	130
МАНЬГОРА В.В. Інформаційно-правове забезпечення юридичної освіти.....	138
МАНЬГОРА Т.В. Набувальна давність на земельну ділянку.....	145

До відома читачів

РЕКОМЕНДАЦІЇ міжнародної науково-практичної конференції на тему: “Система військової юстиції у забезпеченні національної безпеки України”, м. Київ, 29 жовтня 2019 року.....	153
--	-----

РЕКОМЕНДАЦІЇ міжвідомчого “круглого столу” на тему:
“Наукова діяльність та інформація з обмеженим доступом: актуальні проблеми і шляхи їх вирішення”, м. Київ, 14 листопада 2019 року..... **156**

Рецензія на монографію:

“Національна безпека України в інформаційну епоху: правові аспекти”
/ авт. І.М. Доронін; рецензент керівник науково-дослідного центру правового забезпечення інформаційної і національної безпеки НДІП НАПрН України, заслужений юрист України, доктор юридичних наук, професор Є.Д. Скулиш...**159**

До відома авторів.....161

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.

Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 x 108/16. Спосіб друку – різнографія. Ум. друк. арк. 14.3. Тираж 100 прим.

Виготовлено з оригінал-макета в друкарні ТОВ “Видавничий дім “АртЕк”.

04050, м. Київ, вул. Мельникова, буд. 63. Свідectво про внесення суб’єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції – серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІП НАПрН України, протокол № 3 від 20.2.20 р.

TABLE OF CONTENTS

Informative Law

DZOBAN O., RUBAN O. Freedom and responsibility as axiological markers of the transformation of the information society.....	9
RADUTNIY O. Direction of time in the law system	22
BRYZHKO V., PYLYPCHUK V. Privacy, confidentiality and security of personal data.....	33

Legal Informatics

VARAVA I. Innovation in the professional practice of lawyers: utilizing the capacity of artificial intelligence.....	47
---	----

Informative and National Safety

KORZH I. Conceptual principles of legal security.....	55
DORONIN I. Security as essence of state functions.....	66
SOLODKA O. State information sovereignty ensurance: legal discourse.....	80
GUTSALYUK M. Threatening tendencies of organized cyber crime.....	88
PETROV S. Organizational and legal framework for addressing cyber attacks in the European Union.....	99
DOROGIЙ C. Involving citizens in the legislative process: first summary.....	106
BATYRGAREIEVA V. Conceptual model of protection of information space of Ukraine by means of criminal law.....	110

Information on other subject research directions by specializations in the field of knowledge 08 – “Law”

ZHORNIAK A. About approaches to the classification of information services in the field of economy.....	120
GOLOVKO O., DRUZ V. The right to justice and the right to access information: correlation and interdependence.....	130
MANGORA V. Legal and information support for legal education.....	138
MANGORA T. Time of prescription for the land plot.....	145

For the consideration of readers

RECOMMENDATIONS of the International Scientific and Practical Conference on “The system of military justice in national security of Ukraine”, Kyiv, October 29, 2019.....	153
--	-----

RECOMMENDATIONS of the Interagency “Round Table” on “**Scientific Activity and Restricted-Access Information: Current Issues and Solutions**”, Kyiv, November 14, 2019..... **156**

Review of the monograph:

“National Security of Ukraine in the Information Age: Legal Aspects”
/ by I. Doronin; Reviewer Head of Research Center for Legal Support
of Information and National Security of the Scientific research Institute
of informatics and law of the National academy of law sciences
of Ukraine, Honored Lawyer of Ukraine, Doctor of Juridical Science,
Professor Ievhen D. Skulysh..... **159**

For the consideration of authors..... **161**

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 3 dated 20.2.20

Інформаційне право

УДК 316 (477)

ДЗЬОБАНЬ О.П., доктор філософських наук, професор,
головний науковий співробітник НДІП НАПрН України.

РУБАН О.О., кандидат юридичних наук, асистент кафедри цивільного права № 2
Національного юридичного університету імені Ярослава Мудрого.

СВОБОДА Й ВІДПОВІДАЛЬНІСТЬ ЯК АКСІОЛОГІЧНІ МАРКЕРИ ТРАНСФОРМАЦІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Анотація. У статті зроблена спроба уточнити місце свободи й відповідальності у процесах трансформації аксіосфери інформаційного суспільства. Показано, що інформаційне суспільство – це суспільство, в якому відбуваються інтенсивні світоглядні трансформації, де головними цінностями стають інформація, а також пов'язані з нею симулякризація й віртуалізація, що стимулюють зміни аксіологічних пріоритетів, взаємини і комунікації людей, співвідношення свободи й відповідальності. Доводиться, що етичні трансформації інформаційного суспільства найбільше пов'язані з темою соціальної стійкості особистості, яка часто не усвідомлює меж своєї свободи й відповідальності в інформаційному просторі.

Ключові слова: свобода, відповідальність, інформаційне суспільство.

Summary. The article attempts to clarify the place of freedom and responsibility in the process of transforming axiosphere of information society. It is shown that the information society is a society in which there are intense philosophical transformation, where the main values are: information, as well as related simulacrisis and virtualization that stimulate changes in axiological priorities, the relationships and communication of people who value freedom and responsibility. It is proven that ethical transformation of the information society most related to the topic of social sustainability of personality, which often does not realize the limits of their freedom and responsibility in the information space.

Keywords: freedom, responsibility, information society.

Аннотация. В статье предпринята попытка уточнить место свободы и ответственности в процессах трансформации аксиосферы информационного общества. Показано, что информационное общество – это общество, в котором происходят интенсивные мировоззренческие трансформации, где главными ценностями становятся информация, а также связанные с ней симулякризация и виртуализация, стимулирующие изменения аксиологических приоритетов, взаимоотношения и коммуникацию людей, соотношение свободы и ответственности. Доказывается, что этические трансформации информационного общества более всего связаны с темой социальной устойчивости личности, часто не осознающей границ своей свободы и ответственности в информационном пространстве.

Ключевые слова: свобода, ответственность, информационное общество.

Постановка проблеми. Кризу сучасної культурно-цивілізаційної ситуації можна розцінювати, з одного боку, як перехідний період, однак, з іншого – як період, необхідний для вироблення нових ціннісних орієнтирів. У кризовій ситуації можуть виникнути як передумови для виникнення іншої культури, так і передумови, що сприяють загибелі цивілізації в її колишньому вигляді [1, с. 15].

Аксіологічна проблематика, розкриваючи ціннісне ставлення людини до світу, має величезне значення для розуміння сутності і світогляду людини, а характер цінностей визначається спрямованістю суспільних відносин і самоідентифікації особистості [2].

Дзьобань О.П., Рубан О.О.

Проблема цінностей завжди актуальна в перехідні періоди розвитку соціуму. Аксіологічні трансформації, які відбуваються сьогодні, можна інтерпретувати як багатовимірні й різнопорядкові, оскільки у своїй основі вони мають традиційні установки. Внаслідок цього, усвідомлення й осмислення світоглядних змін включає “переоцінку цінностей”, яка може як набувати виду прогресивного заперечення основ попереднього суспільного устрою, так і виражатися в нових формах втілення минулих аксіологічних парадигм.

Звернення до аксіологічних підстав суспільного розвитку набуває виняткової актуальності у наші дні у зв’язку зі зміною світових цивілізацій. Як свідчать результати вітчизняних наукових досліджень історії цивілізацій, зміна світових цивілізацій визначається, насамперед, духовним світом, новими цінностями і новими можливостями людини.

У новому тисячолітті ідея інформаційного суспільства все більш висувається як універсальна ідеологія в умовах глобалізації і наростання комплексу світоглядних проблем, аксіологічних пріоритетів і зростання потреб людей. Формується новий світогляд, в рамках якого значне місце займають віртуальні цінності, зокрема віртуальна свобода й віртуальна відповідальність. Це призводить до трансформації традиційних моральних норм заборонного й дозвольного характеру, до виникнення моральних конфліктів і колізій, що здійснюють суттєвий вплив на духовно-моральний світ людини, її самоідентифікацію.

Результати аналізу наукових публікацій свідчать про те, що проблемам трансформації інформаційного суспільства і його ключових сфер присвячено велику кількість наукових доробків, у яких достатньо ґрунтовно досліджується сутність і особливості вказаного феномена. Разом з тим, комплексному філософському розумінню трансформативних метаморфоз аксіосфери інформаційного суспільства у когнітивному полі “свобода – відповідальність” у наявних наукових публікаціях приділяється недостатня увага.

Метою статті є уточнення місце свободи й відповідальності у процесах трансформації аксіосфери інформаційного суспільства.

Виклад основного матеріалу. Як найбільш важливу рису інформаційного суспільства дослідники виділяють його мережевий характер, який прийшов на зміну колишній стратифікованій структурі, де домінуючі функції і процеси “все більше виявляються організованими за принципом мереж” [3]. Інформаційні технології самі стають додатковим каналом соціальної стратифікації й мобільності. В інформаційному суспільстві формується нова якість індивідуального й суспільного буття, яка полягає у забезпеченні кожної особистості будь-якими знаннями, що, у свою чергу, зумовлює радикальні зміни в усій системі суспільних відносин (політичних, правових, духовних та ін.). Тобто, як слушно вважають деякі вітчизняні дослідники, основна ідея інформаційного суспільства у соціогуманітарному вимірі полягає у досягненні нової фази розвитку – “суспільства знань” і забезпечення для всіх рівного доступу до них [4]. Таким чином, поняття інформаційного суспільства відображає об’єктивну тенденцію у соціальній еволюції, коли інформація (знання) стає однією з основних цінностей у житті людей [5], детермінуючи й трансформуючи розуміння свободи й відповідальності людини.

Визначні характеристики інформаційного суспільства як моделі, є по суті, ідентичними характеристикам постіндустріального суспільства. Головним чинником суспільних змін стає виробництво та використання інформації; теоретичне знання як вища цінність і основний товар стає чинником формування нової соціальної структури

суспільства, а також нових моделей управління. Якщо в індустріальну епоху в умовах капіталістичної економіки вирішальне значення мали власність і капітал, то в інформаційному суспільстві відбувається перехід до обслуговуючої економіки, коли домінуючу роль починає грати сфера послуг, причому послуг передусім інформаційних [6, с. 5].

Отже, зміни, що відбулися в результаті тотальної комп'ютеризації за останні 30 років, виявилися такими глибокими й масштабними, що вони торкнулися серцевини соціального буття, способу життя людей, розуміння ними співвідношення свободи й відповідальності.

В інформаційному суспільстві змінюється уклад життя, система цінностей індивідів і соціальних груп, зростає значущість інформаційних цінностей по відношенню до матеріальних. Це тягне за собою підвищення питомої ваги моральних цінностей і їх віртуальну трансформацію.

Людина техногенної цивілізації розуміється як активно-діяльна істота, перетворювальна діяльність якої є її головним призначенням. При цьому діяльно-активний ідеал ставлення людини до природи поширюється і на сферу соціальних відносин. Для такого суспільства характерним є панування раціонального мислення, націленого на осмислення зовнішнього світу й використання знань для розвитку знарядь виробництва з метою збільшення їх ефективності, а також розуміння природи як об'єктивно існуючої закономірно функціонуючої реальності, пізнавши яку людина як розумна істота може поставити під свій контроль. “Широко відомо, – пише у зв'язку з цим А. Дж. Тойнбі, – що ті індивіди й колективи, зусилля яких повністю зосереджені на перетворенні сировини на світло, тепло, рух і різні предмети споживання, схильні думати, що відкриття й експлуатація природних ресурсів – діяльність, цінна сама по собі, незалежно від того, наскільки цінні для людства результати цих процесів” [7, с. 14]. Виникає машинізована, стандартна, байдужа до національних особливостей і відірвана від спадщини гуманізму масова культура, в якій нівелюються межі свободи й відповідальності, відносини особистої залежності перестають домінувати і підкоряються суспільним зв'язкам, внаслідок чого формуються нові системи цінностей.

В інформаційному суспільстві плюралістичність і мозаїчність життєвих практик і стилів стає визначальною характеристикою. “Все треба спробувати, випробувати: не лише кухню всіх народів, а й культуру, науку, релігію, сексуальність. Число використаних практик може наближатися до нескінченності. Можливі практики нам показують журнали в глянцевиx обкладинках або телекліпи. Цікаво, що виникла потреба може і не проявлятися у формі гострого бажання, специфічної переваги. Найчастіше це – дифузна цікавість” [8, с. 53-54]. Завдяки інформаційній доступності постмодернізм еклектично поєднує у собі досягнення й цінності всіх культурних епох, вільно оперує ними і комбінує їх, маніпулює такими складними компонентами, як мозаїчність, роздробленість образів, знань і цінностей. Поняття “особистість” сьогодні повністю замінено поняттям “маска” [9], тобто, окремий аспект даного феномена стає самим феноменом.

Кардинальні зміни у ставленні людини до світу визначають тенденції переміщення уваги суб'єкта з духовної, інтелектуальної сфери на матеріальну, тілесно-речову, трансформації культу знання й освіти в культ задоволення і природності, звільнення від прагнення до ідеалу на користь прагматизму і утилітаризму, підміни творчості – споживанням, життя – грою, реальних відносин – віртуальними [10 – 11]. Разом з тим, з іншого боку, як справедливо зазначає Н. Ситкевич, “у разі, коли акцент зміщений у бік трансформації старих ціннісних пріоритетів, аксіологічні ефекти інформатизації

включають усвідомлення таких основоположних принципів комунікації як свобода, відповідальність, права людини; перспективи “узгодження” нормативно-ціннісного різноманіття сучасного суспільства пов’язуються з принципами справедливості, гуманності та толерантності” [8, с. 30].

Традиційна філософія трактувала відносини з приводу інформації як суб’єкт-об’єктні, що є характерним для розвитку суспільства з переважанням матеріального виробництва. Тут основна увага приділялася інформації про природну й технічну реальності. У постіндустріальному суспільстві, яке характеризується домінуванням сфери послуг, відносини з приводу інформації зводяться, перш за все, до суб’єкт-суб’єктних відносин. На цьому етапі інформаційна реальність стає все більш важливою для соціальної реальності. В інформаційному суспільстві, де переважає виробництво інформації, виявляється домінування полісуб’єктних (мережевих) відносин. Полісуб’єктність інформаційного суспільства визначається мережевими структурами одночасного обміну інформацією між безліччю різних взаємодіючих суб’єктів. Внаслідок цього формується метаінформаційна реальність другого порядку. Виходячи з цього, інформаційне суспільство можна вважати соціальною формою, що зароджується у постіндустріальній фазі розвитку цивілізації, яка характеризується домінуванням полісуб’єктних (мережевих) відносин.

З мережевим принципом також пов’язані гнучкість і мінливість інформаційного суспільства. При впровадженні низки науково-технічних, соціальних і культурних програм помітно зростає комфортність людського існування, але виникають і негативні прояви як на глобальному, так і на індивідуальному рівні. Здебільшого неусвідомлене бажання володіти матеріальними і соціальними благами, яке формує зовнішнє середовище соціуму, призводить до стагнації внутрішньої духовної сфери, обумовлює приземленість, агресивність інтересів, загрузання у споживання, орієнтація на речі; відчуття й усвідомлення свободи й відповідальності за власні вчинки притупляється; самість розщеплюється від надлишку інформації й комунікацій, виникає відчуття нестійкості, невстигання за змінами, розтрачування сил, втрати пріоритетної орієнтації.

Вітчизняні дослідники інформаційного суспільства та численні дослідники з країн СНД фокусують увагу на тих труднощах і ризиках, з якими стикається сучасна людина, турбуючись найбільше про збідніння її внутрішнього світу, зменшення у ньому частки духовності.

Так, В. Андрущенко, Л. Горбунова, М. Култаєва, С. Пролев та інші науковці стверджують, що сучасне суспільство, створюване глобалізацією і глобальним вільним ринком, характеризується переходом від раціональної утилітарної культури до змішаної глобальної культури; від політичної емансипації до політики “життєвого стилю”; від рівності до відмінностей; від організації, ієрархії до реорганізації, мереж; від фіксованої ідентичності до її плюралізації; від кінця ідеологій до варіації життєвих стилів і переконань [12].

У таких умовах відбувається формування нової людини. Тепер потреби людини розмежовуються на соціально опосередковані, де індивід виступає як вільний член соціуму і демонструє соціально значущу відповідальну поведінку [13], та індивідуально опосередковані потреби, які визначаються виключно суб’єктивними устремліннями до власної реалізації. В. Кремень зазначає, що задоволення індивідуально опосередкованих потреб супроводжується виникненням нових цінностей – довіри, сердечності, ширості, симпатії особистості – тобто цінностей індивідуально-демократичних. Економічні надстатки і ера споживання продовжують проявляти себе як чинник персоналізації та підвищення відповідальності людей, примушуючи до постійної видозміни свого життя.

Споживання розглядається як приклад персоналізації. Мета такого споживання – не тільки гедонізм, але й інформація, інтерес – не лише до насолоди життям, а й до внутрішнього оновлення, а результат – поява поінформованого і наділеного відповідальністю індивіда. У даній ситуації людина стає більш вільною – у реалізації повсякденних потреб, у спілкуванні та освіті, у прагненні до розваг, в моді, в мистецтві, мета яких – звільнення особистого “Я”. Сьогодні успіх асоціюється не з володінням речами, а з якістю життя. Внаслідок цього, саме по собі матеріальне благополуччя втрачає свою значимість, а на перший план виходять проблеми поєднання безпеки і свободи, справедливості й відповідальності. Одночасно перетворення науки і знання на виробничу силу робить очевидною кореляцію між освітою і достатком, підвищуючи соціальний статус їх носіїв. Це у свою чергу змінює ставлення до інформації, у бік якої зміщується споживання, що стимулює генерацію нових знань. Своєрідність цього періоду становить пріоритет індивідуального начала над загальним, психології над ідеологією, різноманіття над однаковістю, свободи над примушенням [14, с. 3].

А. Тадаєва особливо актуалізує увагу на тому, що невід’ємною складовою процесу соціалізації (з усіма її компонентами: адаптація, інтеграція, індивідуалізація) людини інформаційного суспільства в сучасному інформаційному просторі є “медіасоціалізація”, органічною частиною якої є кіберсоціалізація. Остання забезпечує соціальний розвиток людини через Інтернет-простір, впливаючи на якісні зміни структури самосвідомості особистості. Люди різного віку мають неоднакові адаптаційні можливості й по-різному адаптуються до сучасного інформаційного простору. Люди похилого віку є носіями загальнолюдських цінностей, але їм складно адаптуватися до сучасних інформаційно-комунікаційних технологій, повноцінно їх використовувати, що загрожує їх маргіналізацією. Сучасний інформаційний простір розширює професійні можливості дорослих, а відтак – ступінь свободи; молодь є найактивнішою групою, яка використовує нові медіа; діти найлегше використовують всі технічні новинки, вони без труднощів адаптуються до сучасного інформаційного простору, але, не маючи реального соціального досвіду, можуть потрапити в несприятливу ситуацію, втратити органічний зв’язок з системою традиційних цінностей, діяти безвідповідально [15, с. 335].

Практично усі наведені автори сходяться до того, що деградація людини не зупиняється, і цей процес може все інтенсивніше набирати обертів. Звідси виникають проблеми: людина, багато маючи в матеріальному плані, не може досягти внутрішньої гармонії, умиротворення, злагоди з собою. Однією з причин такого стану справ є те, що життя у людини одне і сили її організму не безмежні. Тому, їй рідко вдається однаково активно діяти у багатьох і різних за своїм змістом напрямках і досягати при цьому всюди очікуваного результату. Прийнято вважати, що чим менше хтось розкидається у своїх цілях, думках, контактах, тим більш значущих успіхів він досягає. Наявність свободи волі допомагає людині зробити вибір: або приділяти уваги своєму внутрішньому світу, розвитку духовності, або основні сили спрямовувати у зовнішнє середовище, щоб досягти володіння матеріальними та соціальними благами, настільки активно пропонованими їй у користування інформаційною цивілізацією. Для людини тепер стає настільки характерною заглибленість у світ “речовий”, що її думки обертаються навколо теми придбання товарів, зміцнення фінансової спроможності. А ось усвідомлена необхідність відповідальної життєдіяльності, акти трансценденції, метафізичного здійснення до вищих ідеалів і моральних цінностей зникають з людського буття. Не випадково Ю. Хабермас називає сучасну епоху “постметафізичною” [16, с. 15].

Крім того, пасивне споживання інформації, причому, в цифровому вигляді, все більше витісняє активні форми дозвілля, творчості, пізнання, формує жорсткість мислення, позбавляє людей безпосереднього спілкування один з одним. Звуження персонального простору, відчуження від живої природи викликає мимовільне прагнення до спрощення картини світу, боязнь прийняття рішень, страх відповідальності [17].

Інформаційна цивілізація, до якої дійшло людство, змінює не просто статус інформації, тобто роль її позитивних наслідків, а й різко розширює негативні можливості. Ми отримали сильнодіючий засіб, для якого немає меж. Звідси, з одного боку, роль інформаційних систем і мереж посилює суспільство й державу, з другого – ослабляє, оскільки такі системи і мережі стають основною метою супротивника або опонента. Інформація починає нести в собі як творчу, так і руйнівну силу, що значно посилюється [18, с. 148].

Перетворення в останні десятиліття XX ст. соціальної реальності в нестабільну, фрагментарну, еkleктичну через посилення інформаційних потоків явно корелює зі зростанням у житті людей ролі різного роду симулякрів – образів реальності, що заміщають саму реальність.

Категорію “симулякр” можна визначити як “вислизаючу” від ясного й однозначного тлумачення. Тому її ретельне дослідження, а також вивчення змін в аксіосфері, що відбуваються під впливом процесів симуляції, стає важливим науковим завданням, що має світоглядне й методологічне значення. Виявлення фундаментальних цінностей класичної культури, що зазнають певних труднощів у зв’язку з процесами симуляції, віртуалізації, мережевізації в умовах постійної соціокультурної модернізації, також набуває особливої актуальності [19, с. 67].

Симулякр – це образ відсутньої дійсності, правдоподібна подoba, позбавлена оригіналу, поверхневий, гіперреалістичний об’єкт, за яким не стоїть будь-яка реальність. Це марна форма, автореферентний знак, артефакт, заснований лише на власній реальності. З часів епохи Відродження, пише Ж. Бодрійяр, разом зі змінами закону цінності, послідовно змінилися три порядки симулякрів:

- *підробка* – становить панівний тип “класичної” епохи, від Відродження до промислової революції;
- *виробництво* – становить панівний тип промислової епохи;
- *симуляція* – становить домінуючий тип нинішньої фази, регульованої кодом.

Симулякр першого порядку діє на основі природного закону цінності, симулякр другого порядку – на основі ринкового закону вартості, симулякр третього порядку – на основі структурного закону цінності [20, с. 113].

Ці три порядки надані у його роботі “Символічний обмін і смерть”. У праці “Симулякри і симуляція” Ж. Бодрійяр наводить вже п’ять стадій розвитку феномена симуляції, що прагне до завершеності: він є відображенням базової реальності; він маскує й спотворює базову реальність; він маскує відсутність базової реальності; він не має ніякого відношення до будь-якої якої реальності: він є своїм власним чистим симулякром [21]. Навіть і більше: самі поняття свободи й відповідальності стають симулякрами.

У контексті репрезентативної моделі симулякри як образи, відірвані від дійсності, є невід’ємною стороною комунікативного середовища сучасного соціуму. Як і інші образи, створювані численними інформаційно-комунікативними технологіями кінця XX – початку XXI ст., у тому числі й віртуальної реальності, вони утворюють досить ефективну мотиваційну сферу ціннісної свідомості людини постіндустріальної епохи [22 – 23].

В історичній системі симулякрів, розглянутій Ж. Бодрійяром, панівним типом нинішньої фази розвитку соціуму стає “симуляція”, яка спирається на “структурний закон цінності”, а споживання вивільняється від його звичного значення як “процесу задоволення потреб”, навпаки – сам процес виробництва і споживання активно формує потреби. Споживання, як вважає Ж. Бодрійяр, аж ніяк не є пасивним станом поглинання і присвоєння, який протистоїть стану виробництва, але виступає як активний модус відносин – і “не лише до речей, а й ... до всього світу”, саме в ньому “здійснюється систематична діяльність і універсальний відгук на зовнішні впливи, ...на ньому ґрунтується вся система нашої культури” [21]. Сучасна людина виступає як активна відносно вільна особистість, що проявляє свої особливі, індивідуальні якості у процесі споживання. Поняття “споживання” Ж. Бодрійяр звужує до діяльності систематичного маніпулювання знаками, але не сприймає як матеріальний процес. Зміст речі, ступінь її корисності визначається не споживчою вартістю, досить універсальною, а його високоіндивідуалізованою символічною цінністю. Речі у такій системі відносин не можуть бути порівнянні одна з одною за ознакою еквівалентності, більше того, цінність кожної окремої речі не є закріпленою, але довільно встановлюється в рамках індивідуальної системи потреб.

Досліджуючи цей аспект, філософи розмежували потреби людини на соціально опосередковані (потребую), де індивід виступає як член соціуму і демонструє соціально значуща поведінка, і індивідуально опосередковані (хочу), які визначаються виключно суб’єктивними устремліннями до власної реалізації у споживанні. Задоволення індивідуально опосередкованих потреб супроводжується індивідуалізацією особистості, яка проявляє себе в бажанні людини бути самою собою, виступати “оператором”, який має можливість вільного вибору, бути відмінним від інших індивідів і поведінкою, і смаками, звільнитися від приписуваних суспільством ролей і соціальних правил, нести відповідальність за своє життя і оптимальним чином розпоряджатися своїм естетичним, емоційним, фізичним, емоційним та іншим досвідом, тобто, бути самотійною особистістю. Інтенсифікація подібного прагнення може призвести до надмірного, крайнього індивідуалізму, абсолютизації індивідуальної свободи і виступати смисложиттєвою позицією людини в інформаційній світоглядній парадигмі.

Занепад реальності, описаний Ж. Бодрійяром, означає, що замість “старої” реальності виникає “нова”. В результаті розречевлення суспільство набуває рис, описання яких дає можливість використовувати поняття віртуальної реальності, в яку занурюється людина інформаційного суспільства. Вона починає сприймати світ як ігрове середовище, усвідомлюючи його умовність, керованість його параметрів і можливість виходу з нього. Розрізнення старого і нового типів соціальної організації за допомогою дихотомії “реальне/ віртуальне” дозволяє ввести поняття віртуалізації як процесу заміщення інституалізованих практик симуляціями [10, 24 – 25]. Таким чином, термін “віртуалізація” не тільки виявляється адекватним феноменам, описуваним як інформатизація та розречевлення, але навіть постає як більш евристичне, аніж два останніх концепти, оскільки відкриває перспективу концептуалізації не “кінця” або “зникнення” попереднього суспільства, а процесу формування нового. З цього можна припустити, що віртуалізується не тільки соціум, у якому віртуалізуються свобода й відповідальність, а й породжена цим соціумом особистість [11; 19; 26].

Отже, інформаційне суспільство стає схожим на віртуальну реальність і може описуватися за допомогою її характеристик [27]. Віртуалізація у даному випадку – це будь-яке заміщення реальності її симуляцією із застосуванням логіки віртуальної реальності. Результатом подібного ретушування меж діяльнісного ареалу людини стає емоційна

нестабільність, прагнення прикритися грою, запереченням ієрархій, безтурботними веселощами. Крім того, відбувається зміщення центру внутрішнього духовного світу в бік культу тіла як найбільш очевидної й непереборної цінності. Для тілоцентризму виявляється характерним перехід від слова до тіла, від інтелектуальності й духовності до тілесності, від вербальності до зорового образу, від раціональності до “нової архаїки”, коли в центрі ментальності виявляється тіло, плоть. Також виникає підвищена увага до катастроф, апокаліптичних сюжетів – усього того, що може зруйнувати тіло і до того, що забезпечує тілесне задоволення (сексуальна свобода, наркотики, розваги, що ведуть до зміни відчуттів). Сучасні рекламні технології лише підсилюють такі інтенції, активно експлуатуючи й культивууючи зображення і практики тіла [28 – 29].

У сучасному світі найважливішою об’єктивною обставиною становлення людини виявляється інформаційна доступність, яка трактується як загальна інформаційна прозорість, максимальна інформаційна насиченість, інтенсивність інформаційних потоків і фантастично швидкоплинна їх зміна. В інформаційному суспільстві всі люди виступають споживачами масової інформації – зараз практично кожен підключений до інформаційних мереж так само, як до житлово-господарських комунікацій; радіо, телебачення, газети, телефон, персональні комп’ютери несуть масу інформації кожній родині. Споживач інформації перетворюється на ненаситного поглинач інформації.

Індивідуальна, групова й масова свідомість в дедалі більшою мірою піддається агресивним інформаційним впливам, що завдає шкоди психологічному і моральному здоров’ю населення, руйнує моральні норми життя і призводить до дестабілізації соціальної ситуації. Для розуміння механізмів інформаційного впливу на масову, групову та індивідуальну свідомість доцільно звернутися до категорії “інфологема” (*термін В. Когана*) – неякісна або помилкова інформація, створювана для заміщення базових фактів артефактами. Інфологеми з’являються як результат неусвідомлюваних помилок або свідомих, цілеспрямованих маніпулятивних впливів. Вони мають здатність до розширеного відтворення, самопримноження і об’єднання в системи. Інфологеми впливають на людину протягом практично необмеженого часу, оскільки легко потрапляють в інформаційний фонд та тезауруси, стають їх елементами і як такі беруть участь у формуванні спотвореної картини світу. Засоби й методи маніпулятивних впливів на людину стають більш витонченими і застосовуються повсюдно. У людини, об’єкта маніпулювання, формується почуття практично безмежної свободи, створюється враження, що вона сама керує своєю поведінкою, здійснюючи усвідомлений вибір на основі раціонального аналізу ситуації. Інфологеми формують стійкі стереотипи індивідуальної та соціальної поведінки і здатні дезорієнтувати цілі покоління, призвести до нівелювання ціннісних систем. Значна частина соціально-психологічних інфологем має у своїй основі єдність двох властивих людині особливостей: ксенофобії, ненависті до іншого (чужинця) і прагнення знайти ворога – винуватця всіх негараздів.

В інформаційному просторі у величезних кількостях і з небаченою швидкістю продукуються соціальні, політичні, художні, релігійні міфи, і, як факти соціального життя, незважаючи на свій ілюзорний характер, здійснюють цілком реальний вплив на суспільство. Новий міф перетворився на засіб соціальної мобілізації та маніпуляції суспільною свідомістю. Сучасна культура продовжує інтенсивно продукувати міфи, покликані зв’язувати й каналізувати суспільну енергію, задовольняти запити суспільства хибними цінностями масового споживання, наприклад, простимулювати споживання продуктів, як це робить реклама, створити за допомогою телебачення привабливий імідж політичного діяча або естрадної “зірки”, зайняти увагу глядача черговим бойовиком або “мильною оперою” за допомогою кінематографа й телебачення.

Новий міф виступає у вигляді неправдивої мобілізуючої структури, здатної безболісно вписувати людину й маси у соціальну реальність, створюючи при цьому у своїх adeptів враження істинності і стану психологічного комфорту. Так, наприклад, настільки широко впроваджена в масову свідомість телевізійна реклама здійснює значний вплив на культурно-інформаційний простір, що створюється нею, багато в чому за принципом міфологізації дійсності. Інформація, оформлена в оболонку міфу, набуває чуттєво-виразної конкретності, легко запам'ятовується, естетизує життєвий світ сучасної людини і кидає її, в кращому випадку, в обійми ілюзій, а в гіршому – робить об'єктом різних маніпуляцій, у тому числі й політичних [30].

Варто зазначити, що інформаційне суспільство – саме по собі деякою мірою є соціальним міфом, привабливість якого в тому, що він експлуатує таке найбільше науково-технічне досягнення, як інформаційно-комп'ютерні комунікації. Чарівність міфу інформаційного суспільства така, що проти нього не встояли не тільки кібернетики та інформатики (нерозумно відмовлятися від такої розкішної реклами), але й гуманітарії, почесне місце яким у цьому гіпотетичному суспільстві зовсім не гарантоване. Справа в тому, що в інформаційному суспільстві знецінюються усталені традиційні освітні, пізнавальні та інші цінності і дедалі більшим попитом користуються не інтелігенти, а інтелектуали-технократи, які зорієнтовані на особистий успіх. Інформаційні потреби інтелектуалів будуть задовольняти глобальні електронні павутини, а не книги.

Втрата приватності, характерна для активної діяльності інформаційних мереж, створює основу для процесу уніфікації особистості й деперсоналізації. Інформаційна відкритість не тільки не перешкоджає індивідуалізації, але також сприяє впровадженню у свідомість безпрецедентно масових стандартів, які часто на узгоджуються з традиційними уявленнями про свободу людини і її відповідальність за результати своєї діяльності.

Людина в усі часи у своїй діяльності надихалася певним колом ідей та цінностей, що генеруються загальновизнаними героями. Дослідники констатують, що сьогодні місце героїв зайняли так звані квазісуб'єкти – віртуальні збірні стереотипи, які активно культивуються, найчастіше, політичною та торговою рекламою. Як справедливо стверджує Д. Іванов, у рекламних кліпах конструється квазісуб'єкт, який нібито й робить правильний вибір [27]. Таким чином, формуються ціннісні стереотипи, починаючи від рівня здорового способу життя до соціальної спрямованості й мотивації, а сучасні герої-квазісуб'єкти проповідують головну сучасну цінність – споживання.

У традиційному та індустріальному суспільствах переважною формою комунікацій була аксіальна комунікація (що з'єднує тих, хто відправляє й отримує точно адресоване повідомлення), і, відповідно, сфера спілкування була, перш за все, сферою циркуляції сигналів особистої спрямованості. У постіндустріальному суспільстві ситуація змінюється: сигнали колективної спрямованості визначають сферу спілкування кожної конкретної людини. Індивід постмодерну – це людина, що існує в системі ретельної комунікацій (яка не має строго визначених суб'єктів спілкування). Це нове середовище спілкування формує сучасна масова культура, ЗМІ, реклама тощо. Сьогодні практично знецінилося живе індивідуальне спілкування: майже ніхто не звертається до людини індивідуально. Прийнято звертатися до цілих груп, субкультур, носіїв єдиного стилю (“шановні телеглядачі”, “радіослухачі”, “панове”). Людина все більше спілкується не з реальними людьми, а з квазісуб'єктом – віртуальним усередненим типом, який синтезує у собі характерні риси безлічі людей [31]. Звідси – відчуття повної свободи, неконтрольованості, безвідповідальності сучасної людини.

Теоретики постіндустріалізму виходять з того, що у повсякденній свідомості в силу об'єктивних обставин смисложиттєві питання вже не перебувають у конкретно-практичній площині – людина позбавлена необхідності постійно працювати, щоб підтримувати життя тіла, продовження роду також перестає бути незаперечною домінантою. Дійсна унікальність сучасної ситуації полягає в тому, що питання про сенс життя прирівняли до питання: “Як витратити величезну масу вільного часу?” [8, с. 64].

Якщо “звільнені” від роботи люди отримують від суспільства необхідні їм засоби для життя, явище це в принципі можна оцінювати позитивно. Але це лише одна сторона медалі, є й інша. Людина, добровільно або недобровільно втрачаючи роботу, втрачає тим самим і своє основне, притаманне більшості людей уявлення про сенс життя як постійної трудової діяльності для підтримки свого власного існування і забезпечення своїх близьких. Вихід з цієї скрутної ситуації теоретики постіндустріалізму вбачають у зміні провідного типу діяльності: навчання замість праці. Безперервне становлення, саморозвиток особистості – все це має стати головною ідеєю людини постіндустріального суспільства. Так, А. Шафф пропонує докласти зусиль для цілеспрямованого формування нових типів людини – *Homo Studiosus* і *Homo Universalis*. Людина “Універсальна” розуміється ним як всебічно освічена, спроможна до зміни професії і тим самим – позиції в суспільному розподілі праці. Крім того, він зауважує, що людина інформаційного суспільства знаходиться у стані цейтноту, в стані гравця, якому загрожує програш, оскільки йому залишилося занадто мало часу для того, щоб зробити необхідну кількість ходів, необхідних для зміни природи людини. Усе це вимагає величезної підготовчої роботи й осмислення, які ще й не почалися, а “час не чекає, якщо ми не хочемо створити соціальну патологію” [32, с. 319-320]. Цим А. Шафф визнає існування певної загрози внутрішнього стану особистості в нових умовах.

Наявність у людини засвоєного нею сенсу життя є позитивною цінністю, оскільки визначає навіть її психічне здоров'я. Сучасна економіка споживання несе в собі елементи, що представляють загрозу цій цінності і психічному життю людей. Загроза ця пов'язана з іманентно властивим постіндустріальному суспільству структурним безробіттям в результаті автоматизації та роботизації. Робота завжди виступала символом самостійності, соціальної повноцінності, інструменту соціальної самоідентифікації, шляхом до відповідного соціального статусу, без чого зникає стимул і в життя закрадається нудьга – в сенсі повної відсутності інтересу до всього, чим живе суспільство. Оскільки головним “інстинктом” сучасної людини є споживання, то й порожнечу, яка виникла внаслідок відмирання звичного уявлення про сенс життя, вона заповнює споживанням – споживанням продукції індустрії розваг. Цей яскравий калейдоскоп ілюзорних ігор спроможний повністю або частково дезорієнтувати свідомість “розмити” усвідомлення цінності того чи іншого феномена, тієї чи іншої речі. Без серйозної та відповідальної роботи людина поступово втрачає розуміння реальності. Світ навколо настільки мозаїчний і в той же час привабливий, що увага постійно розщеплюється, а особистісний світогляд вже більше не являє собою цілісну гармонійну систему.

Засоби масової комунікації (як відображення, провідник інформації) на рівні віртуальної реальності стали відтворювати складні структури і порядки і впливати на світ об'єктивної реальності, не тільки відображаючи, а й конструюючи його на свій розсуд. Вони повсюдно занурюють людину не в об'єктивну інформацію, тобто в незалежні за змістом від бажання і волі людей зв'язки і відносини [33], а у віртуальну реальність, у віртуальні об'єктивовані зв'язки й відносини, у віртуальну інформацію, що представляє собою “вторинну інформацію” – опредметнені матеріалізовані людські знання, цінності, ідеали, інтереси тощо. У цих, віртуальних об'єктивних зв'язках і

відносинах є інше – нове, багато в чому нам ще не зрозуміле звучання (поняття, зміст) і цілей, і ідеалів, і обов’язків, і справедливості і інших суб’єктивних проявів. У принципі, суспільство інформаційних комунікацій – це прорив людини в царину багато в чому для нас невідомого, але вже і зараз очевидно – багато в чому й небезпечного [8, с. 38].

Поява електронних комунікацій створила чимало можливостей для інформаційно-пізнавального розвитку людини, але разом з тим, ці комунікації саме цією “вторинною” віртуальною інформацією сковують розум людини. Вона, як справедливо зазначає В. Кутирєв, може (прагнути) замикатися в горизонті віртуальної реальності, і важко її покинути, аж до божевілля [34]. У цьому сенсі віртуальна реальність втягує людину у світ ілюзорної інформації та реальності, в якій вона шукає порятунку, але яка таїть у собі небезпеку, спричинену стійкою залежністю. Але небезпека занурення у таку реальність полягає ще й у тому, що в такій ситуації людина не прагне до осмислення потоків інформації, які часто не мають ціннісної наповненості, глибокого аналізу і не вимагають від неї зробити свідомий інформаційний вибір з етичної точки зору. Це, у свою чергу, обумовлює і віртуальну (ілюзорну за змістом) поведінку суб’єкта – активність без можливості відповідальності за прийняте рішення.

Висновки.

Отже, підсумовуючи сказане, зазначимо, що причиною віртуалізації інформаційного суспільства є об’єктивна потреба у переході інформаційних технологій на новий якісний рівень, а також іманентна людині ціннісно наповнена потреба у творчості, у створенні нової реальності, таких світів, по відношенню до яких вона була б творцем, відчувала максимальну свободу. Подібні діяльні інтенції, що базуються на віртуалізації інформації, визначають її ціннісну рефлексію і відбір з позицій людиновимірності. Ведучи мову про структурні складові суспільства, слід зазначити, що суспільство – це, перш за все, люди, кожна людина зокрема, яку завжди цікавила і буде цікавити вона сама. Для того, щоб людина могла самовизначитися у суспільстві, бути вільною, їй необхідні внутрішні критерії, тобто система цінностей, ціннісних орієнтацій. Остання визначає змістовну сторону спрямованості особистості і складає основу її ставлення до навколишнього світу, до інших людей, до себе самої, основу світогляду і ядро мотивації життєвої активності, основу життєвої концепції і філософії життя.

Етичні трансформації інформаційного суспільства найбільше пов’язані з темою соціальної стійкості особистості, яка часто не усвідомлює межі своєї свободи й відповідальності в інформаційному просторі, оскільки: а) не готова до цієї свободи і, тим більше, до відповідальності емоційно та інтелектуально; б) не сформувала на сьогодні відповідні алгоритми структурування та критичного осмислення інформації, які, знов-таки, мають співвідноситися зі сформованими аксіологічними комплексами.

Інформаційне суспільство – це суспільство, в якому відбуваються інтенсивні світоглядні трансформації, де головними цінностями стають інформація, а також пов’язані з нею симулякризація й віртуалізація, що стимулюють зміни аксіологічних пріоритетів, взаємини і комунікації людей, співвідношення свободи й відповідальності. При цьому, сама цінність людської особистості знижується за рахунок превалювання аспектів утилітарності і прагматичності, як в контактах, так і в тій інформації, якою людина оперує.

Використана література

1. Сучасне суспільство: філософсько-правове дослідження актуальних проблем: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. Харків: Право, 2016. 488 с.

2. Dzeban O., Aleksandrova O., Vinnikova N. Axiological portrait of information society. *Схід: аналітично-інформаційний журнал*. 2019. № 5 (163). С. 13-19.
3. Костина А.В. Тенденции развития культуры информационного общества: анализ современных информационных и постиндустриальных концепций. URL: [http://www.zpu-journal.ru/e-zpu/2009/4/kostina information society](http://www.zpu-journal.ru/e-zpu/2009/4/kostina%20information%20society) (дата звернення 12.10.19).
4. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д.ф.н., проф. В.Г. Воронкової. Запоріжжя: Вид-во ЗДІА, 2017. 292 с.
5. Дзьобань О.П., Кальницький Е.А. Зародження концептуальних підходів до розуміння сутності і специфіки інформаційного суспільства. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. 2013. Вип. 5 (19). С. 3-15.
6. Дубов Д.В., Ожеван М.А., Гнатюк С.Л. Інформаційне суспільство в Україні: глобальні виклики та національні можливості. Київ: НІСД, 2010. 29 с.
7. Тойнби А. Дж. Постижение истории: сборник. Москва: Прогресс-Культура, 1996. 606 с.
8. Ситкевич Н.В. Особенности трансформации нравственных ценностей в условиях информационного общества: этико-философский анализ: дис. ...канд. филос. наук. Новомосковск, 2011. 139 с.
9. Савченко А.А. Постмодернізм як соціокультурне явище. *Вісник Харківської державної академії культури*. 2011. Вип. 33. С. 196-202.
10. Дзьобань О.П., Мелякова Ю.В. Раціональні засади віртуальної реальності. *Політологічний вісник: збірник наукових праць*. 2012. Вип. 59. С. 8-15.
11. Дзьобань О.П., Соснін О.В. Віртуальна реальність суспільства постмодерну як соціокультурне зло соціалізації "людини інформаційної". *Гуманітарний вісник Запорізької державної інженерної академії: збірник наукових праць*. 2017. Вип. 69 (1). С. 69-76.
12. Філософія і методологія розвитку вищої освіти України в контексті євроінтеграційних процесів / В. Андрущенко, Л. Горбунова, М. Култаєва, С. Пролев та ін. Київ: Педагогічна думка, 2011. 320 с.
13. Дзьобань О.П., Рубан О.О. Відповідальність: до проблеми концептуалізації категорії. *Інформація і право*. № 4(31)/2019. С. 9-19.
14. Кремень В.Г. Інноваційна людина і сучасна освіта. *Вісник Чернігівського національного педагогічного університету. Педагогічні науки*. 2013. Вип. 110. С. 3-5.
15. Тадаєва А.В. Особливості соціалізації людини в сучасному інформаційному просторі. *Теоретико-методичні проблеми виховання дітей та учнівської молоді*. 2013. Вип. 17 (2). С. 329-337.
16. Хабермас Ю. Будущее человеческой природы. На пути к либеральной евгенике? / пер. с нем. М. Л. Хорькова. Москва: Весь Мир, 2002. 143 с.
17. Дзьобань О.П., Пилипчук В.Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія / за заг. ред. проф. В.Г. Пилипчука. Харків: Майдан, 2011. 244 с.
18. Дзьобань О.П., Панфілов О.Ю., Соболева С.М. Інформаційне насильство: змістовний аспект. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія*. 2016. № 1 (28). С. 136-151.
19. Данильян О.Г., Дзьобань О.П. "Симулякр": концептуалізація феномена у постнеокласичній філософії. *Інформація і право*. № 2(17)/2016. С. 66-76.
20. Бодрийяр Ж. Символический обмен и смерть / пер. с фр. С.Н. Зенкина. 3-е изд. Москва: Добросвет; КДУ, 2009. 389 с.
21. Бодрийяр Ж. Симулякры и симуляция. URL: http://lit.lib.ru/k/kachalow_a/simulacres_et_simulation.shtml (дата звернення 07.03.2020).
22. Дзьобань О.П. Філософія інформаційних комунікацій: монографія. Харків: Майдан, 2012. 224 с.
23. Дзьобань О.П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади: монографія. Харків: Майдан, 2013. 360 с.

24. Дзьобань О.П., Жданенко С.Б. Віртуальна реальність: метафізичний сенс. *Вісник Національної юридичної академії України імені Ярослава Мудрого. Серія: Філософія, філософія права, політологія, соціологія*. 2012. Вип. 2 (12). С. 97-104.
25. Дзьобань О.П., Жданенко С.Б. Віртуальні комунікації: роль і місце у сучасному світі. *Правова інформатика*. № 2(46)/2015. С. 9-16.
26. Дзьобань О.П. Діалектика глобалізації віртуальної реальності й суспільного розвитку. *Гілея: збірник наукових праць*. 2012. Вип. 63 (№ 8). С. 254-260.
27. Иванов Д.В. Виртуализация общества: Версия 2.0. Санкт-Петербург: ПВ, 2002. С. 29-34.
28. Карповець М. Тіло, мода, ідентичність: постмодерні конфігурації. *Наукові записки Національного університету "Острозька академія". Філософія*. 2013. Вип. 14. С. 156-160.
29. Шкіль Л.Л. Тілоцентризм як нове явище Постмодерну. *Гілея: збірник наукових праць*. 2015. Вип. 94. С. 169-172.
30. Дзьобань О.П. Сучасний віртуальний простір: конгеніальність віртуальності й міфу. *Стратегічні пріоритети. Серія "Філософія"*. 2017. № 3. С. 163-170.
31. Ігнатенко В. Самотній квазісуб'єкт у епоху постмодерну: критика глобалізованого суспільства. *Вісник Національного авіаційного університету. Серія: Філософія. Культурологія*. 2011. № 2. С. 88-93.
32. Шафф А. Куда ведет дорога? Философия истории. Антология. Москва: Аспект-Пресс, 1995. С. 311-321.
33. Никитин Л.Н. Виртуальность – этап или тупик ноосферы? *Творческое наследие В.И. Вернадского и современность: сб. трудов Международной конференции, м. Донецк, 10-12 апреля 2001 г. Донецк: "Донбасс", 2001. С. 373-377.*
34. Кутырев В.А. Оправдание бытия. URL: <http://www.elcom.ru/~human/kutyrev/opravdanie.html> (дата звернення 07.03.2020).

~~~~~ \* \* \* ~~~~~

УДК 115.4:343.211

**РАДУТНИЙ О.Е.**, доктор філософії (Ph.D.) з юридичних наук, доцент,  
доцент кафедри кримінального права № 1  
Національного юридичного університету ім. Ярослава Мудрого.  
ORCID: <https://orcid.org/0000-0002-6521-3977>.

## НАПРЯМОК ЧАСУ В СИСТЕМІ ПРАВА

**Анотація.** В статті здійснено спробу поставити питання щодо можливості зміни напрямку вектору часу від майбутнього до минулого в площині права. Проведена наукова розвідка виявила факти нелінійності розгортання окремих обов'язкових ознак об'єктивної сторони певних складів злочинів, зокрема, простору як місця вчинення злочину, часу, способу тощо. За допомогою прикладів доведено можливість продовження реалізації у часі та просторі інших, крім діяння та наслідку, обов'язкових ознак об'єктивної сторони кримінального правопорушення вже після того, як настав момент його закінчення. Автор приходить до висновку, що час у кримінальному праві є реляційною категорією, і це допускає залежність його характеристик від характеру та способу взаємодії об'єктів, подій, властивостей та відносин. Час у праві може бути визначений за допомогою не однієї, а декількох величин, він може бути ізотропним, тобто рівноправним у всіх своїх можливих напрямках руху. Напрямок руху часу в системі права може змінюватися. У праві майбутнє може впливати на минуле. Інше парадоксальне пояснення може полягати у тому, що певна передбачена чинним законодавством подія у майбутньому здатна перекроїти простір і час у минулому таким чином, що вчиненого злочину ніколи не було. З іншого боку, можливо, що проведені дослідження у черговий раз підкреслює умовність всього того, що відбувається у царині права.

**Ключові слова:** право, кримінальне право, час, простір, напрямок часу, злочин, об'єктивна сторона злочину, минуле, майбутнє, світова лінія, вплив майбутнього на минуле

**Summary.** The article attempts to inquire about the possibility of changing the direction of the time vector from the future to the past in the field of law. Research has revealed the facts of the nonlinearity in deployment of certain crime. The examples demonstrate the continuing possibility of the criminal offense realization after the moment of its termination. The author concludes that time in criminal law is a relational category, and this allows the dependence of its characteristics on the nature and manner of interaction of objects, events, properties and relationships. Time in the field of law can be determined by several quantities. Time in the field of law can be isotropic, that is, equal in all its possible directions of motion. The direction of time progression in the field of law may change. In the field of law, the future can affect the past. Another paradoxical explanation may be that a certain event, envisaged by current law, is capable of reshaping space and time in the past in such a way that no crime has ever been committed. Or, once again, the research underlines the arbitrariness of all that is happening in the realm of law.

**Keywords:** law, criminal law, time, space, direction of time, crime, objective side of the crime, past, future, worldline, impact of the future on the past

**Аннотация.** В статье предпринята попытка поставить вопрос о возможности изменения направления вектора времени от будущего к прошлому в сфере права. Проведенное исследование выявило факты нелинейности развертывания отдельных обязательных признаков объективной стороны конкретного состава преступления, в частности, пространства как места совершения преступления, времени, способа и т.п. С опорой на примеры доказана возможность продолжения реализации во времени и пространстве иных, кроме деяния и последствия, обязательных признаков объективной стороны преступления уже после того, как наступил момент его окончания. Автор приходит к выводу о том, что время в уголовном праве

является реляционной категорией, и это допускает зависимость его свойств от характера и способа взаимодействия объектов, событий и отношений. Время в сфере права может быть определено не только с помощью одной, но и нескольких величин, оно может быть изотропным, то есть равноправным во всех своих возможных направлениях движения. Направление движения времени в системе права может меняться. В сфере права будущее может влиять на прошлое. Иное парадоксальное объяснение может заключаться в том, что определенное предусмотренное действующим законодательством событие в будущем способно перекроить пространство и время в прошлом таким образом, что совершенного преступления никогда не было. Так же не исключается, что проведенное исследование в очередной раз подчеркивает условность всего того, что происходит в области права.

**Ключевые слова:** право, уголовное право, время, пространство, направление времени, преступление, объективная сторона преступления, прошлое, будущее, мировая линия, влияние будущего на прошлое

**Постановка проблеми.** На підставі закону збереження енергії будь-яке суспільно небезпечне діяння завжди породжує суспільно небезпечний наслідок, адже викликана першою з вказаних подій соціальна хвиля (коливання) не може не створювати певні зміни в оточуючому їх просторі та відносинах між певними суб'єктами. Маючи на меті сформулювати заборонену або небажану поведінку, законодавець завжди описує саме діяння, але не у кожному випадку вказує на наявність конкретного наслідку. У такий спосіб відбувається нормативна побудова злочинів з матеріальним, формальним або усіченим складом. Втім, якщо стане можливим виявити та неодноразово підтвердити однаковими експериментальними повторами приклади того, що третя подія, яка також полягатиме у певній поведінці, матиме здатність змінювати попередні (діяння та(або) його наслідок, який вже фактично настав незалежно від того, виявлений він або ні, описаний він у складі певного правопорушення або ні), то такий феномен стане вагомим аргументом проти непохитного переконання про спрямованість часу лише в один бік, а саме – від минулого до майбутнього.

Відомо, що середньовічна індульгенція надавала у певних випадках можливість спочатку покаятися за неіснуючу провину, а вже потім сотворити відповідний гріх, тобто, поміняти місцями порушення та відплату за нього. Але класичний умовивід про неможливість безкарного вчинення вбивства після повного відбуття суворого покарання за те, що його не вчиняв (невинна людина відбула покарання внаслідок судової помилки, наклепу, підроблення доказів обвинувачення тощо), завжди лінійно призводив до наслідків, які є несприятливими для обуреної загальною несправедливістю особи: фактично вчинене вбивство, навіть після безпідставного відбуття покарання за такий самий злочин, не виключає кримінальної відповідальності.

Але якщо час спливає не тільки від минулого до майбутнього, але й навпаки, з чим вже фактично погоджується сучасна квантова фізика, то це не може не мати певного значення та несподіваних наслідків для права у цілому та кримінального, зокрема.

**Результати аналізу наукових публікацій.** Питання взаємозалежності часу, простору, матеріальних об'єктів та правовідносин були і залишаються предметом аналізу практично для кожного з філософів, починаючи з Левкіппа та Фалеса Мілетських, Піфагора, Демокріта, Епікура, Арістотеля, Птолемея і багатьох інших. Вагомі внески у дослідження феномену часу у межах складу злочину здійснені в роботах М.І. Бажанова, Ю.В. Бауліна, В.І. Борисова, Л.П. Брич, Н.О. Гуторової, Л.М. Демідової, О.О. Дудорова, З.А. Загінєй (Тростюк), Ю.Ю. Коломієць, А.А. Музики, В.О. Навроцького, М.І. Панова, Ю.А. Пономаренко, В.В. Сташиса, Є.Л. Стрельцова,

В.Я. Тація, В.О. Тулякова, П.Л. Фріса, В.І. Шакуна, М.І. Хавронюка, В.Б. Харченко та багатьох інших.

Але питання щодо можливості впливу майбутнього на минуле в площині права, або більш вузько – кримінального права, поки що не розглядалося в жодній з відомих публікацій в контексті поглядів сучасних наук, в тому числі квантової фізики, на час і простір.

**Метою статті** є формулювання і аргументування гіпотетичного припущення щодо спостереження, фіксування та аналізу окремих випадків зміни напрямку вектору часу від майбутнього до минулого в царині, зокрема, на прикладі кримінального права.

**Виклад основного матеріалу.** Частиною 5 ст. 212 КК України передбачено, що діяння, описані частинами першою, другою або третьою цієї статті, не вважаються умисним ухиленням від сплати податків, зборів (обов'язкових платежів), якщо платник податків досяг податкового компромісу відповідно до положень підрозділу 9-2 розділу ХХ “Перехідні положення” Податкового кодексу України. При цьому особа не звільняється від відповідальності (ч. 4 ст. 212 КК України), або покарання та його відбування (ст.ст. 74 – 87 КК України), можливість для добровільної відмови (ст. 17 КК України) вже втрачено у зв'язку з наявністю усіх ознак складу злочину, завдяки чому злочин вважається закінченим (ч. 1 ст. 13 КК України). Декриміналізації теж не відбулося. Але вчинене у минулому не вважається злочином через те, що подія у майбутньому (досягнення податкового компромісу) якимось чином змінила його на суспільно корисну або суспільно нейтральну поведінку, адже інших варіантів фактично не існує. За такою законодавчою конструкцією стає можливим через подію у майбутньому вплинути на подію у минулому, отже, змінити підхід до лінійного протікання часу лише в одному напрямку та його відповідного сприйняття. З цього може випливати наступний парадоксальний висновок: певна передбачена чинним законодавством подія у майбутньому здатна перекроїти простір і час у минулому таким чином, що вчиненого злочину ніколи не було.

У зв'язку з цим виникає потреба уважніше придивитися до окремих особливостей феномену часу.

За допомогою категорії часу відбувається опис розвитку причинно-наслідкового зв'язку, коли одна подія поступово переходить у наступну і вони обидві пов'язані між собою загальною енергетичною єдністю. Час є однією з фундаментальних координат простору-часу, вздовж яких розміщуються світові лінії всіх фізичних (матеріальних) тіл.

Поняття “світова лінія” (worldline), що описує унікальну подорож конкретного об'єкту через чотирьохвимірний просторово-часовий континуум, було введено до термінологічного апарату фізики Альбертом Ейнштейном і сьогодні воно найбільш часто використовується в теорії відносності, зокрема в загальній та спеціальній її частинах. У широкому тлумаченні це поняття застосовується для представлення будь-якої послідовності подій, його використання не обмежується будь-якою конкретною теорією. Так, світовою лінією є послідовність особистих подій окремої людини від моменту та місця її народження до моменту і місця смерті, записи у бортовому журналі транспортного засобу про послідовну з плином часу зміну ним певного географічного положення тощо.

У праві також існує можливість спостерігати світові лінії. Так, світова лінія об'єктивної сторони окремого злочину у межах понятійного апарату кримінального права може проявлятися як певний акт поведінки, вчинений у передбачений законом спосіб, з урахуванням місця, обстановки, часу, використаних знарядь та інших матеріальних об'єктів або обставин. Як було зазначено вище, такий акт суспільно

небезпечної поведінки обов'язково викликає за собою певний суспільно небезпечний наслідок. Описаний акт з усіма своїми елементами розгортається в часі як процес, що має власну динаміку, тобто початок і розвиток (наприклад, процес поступового позбавлення життя іншої людини), закінчення (яке, насправді, не є перериванням загального ланцюжку, але лише перетіканням одного в інше) та статику, що має правове значення (наприклад, наслідок за ст. 115 КК України у вигляді позбавлення життя, тобто спричинення смерті іншій людині).

У класичній фізиці час є неперервною величиною. На сьогодні нам не є відомим, чим саме зумовлений час. Він вважається однією з апіорних характеристик всесвіту, тобто тих, знання про які завжди передують досвіду ("апіорі", від лат. *a priori* – "первісно", "саме собою зрозуміло"). Для вимірювання часу за основу приймається певна послідовність подій, про які є достовірно відомою їх періодичність, тобто повторюваність.

Таку саму роль відіграє час і у квантовій механіці. Але попри квантування (тобто, здійснення переходу від класичного опису фізичної системи до її квантового опису) майже всіх величин (ширина, висота, довжина), час, тим не менш, залишається неквантованим параметром. Питання про те, чи є можливим квантування в галузі права, ще потребує свого дослідження. В класичній фізиці та у квантовій механіці швидкість, з якою спливає час та, головне, напрямок його руху, є сталими і не можуть залежати від подій, явищ та параметрів інших об'єктів.

Втім, зазначена закономірність вважалася аксіоматичною лише до того моменту, поки класичні закони не почали розглядатися як випадок квантових постулатів, що базуються на принципі невизначеності. На підставі останніх час вже не є подібним до прямої залізничної колії, якою можна рухатися лише в один бік та в якій відсутні петлі і відгалуження для повернення на попередню станцію. Для правників важливим і цікавим є питання про те, чи можливо у площині права вчинити певний акт поведінки для того, щоб повернутися на попередню станцію подій та змінити минуле.

У межах спеціальної теорії відносності час почав сприйматися як частина єдиного простору-часу, а не щось самостійне та відокремлене. Тому вважається, що час не може не зазнавати змін, якщо змінюється весь пов'язаний з ним просторово-часовий континуум. Поряд з трьома координатами, такими як довжина, висота та ширина, час є четвертою, яка виявляється не тільки самостійною, але й доволі впливовою, а швидкість його протікання є залежною від системи відліку та від спостерігача [3, с. 209-214]. У загальній теорії відносності швидкість часу додатково залежить ще й від впливу гравітаційних сил.

Поки що відсутні відповіді на питання, якою є природа часу, чому вона є безупинним, а не дискретним, чому ми живемо у світі з одновимірним часом тощо. Але спроби їх розв'язати вже пропонуються у сучасній математичній фізиці (Г. Джеффріс, І.М. Зашкільняк, В.М. Колісник, П.П. Костробій, С.С. Піх, О.М. Попель, М. Рід, А.А. Ровенчак, Ю.К. Рудавський, Б. Саймон, А.В. Свідзинський, Б. Свірлс, І.І. Тальянський, В. Тірінг, М.А. Сухорольський та інші).

Значна більшість дослідників вважали і вважають, що різниця між минулим і майбутнім є принциповою, оскільки інформація переноситься з минулого в майбутнє, але не навпаки. У підтвердження цього наводиться другий закон термодинаміки про послідовне збільшення ентропії у напрямку від минулого до майбутнього. На прикладі це виглядає таким чином, що порцелянова чашка може впасти зі столу і побитися на шматки, але не може зібратися до купи та стрибнути назад на поверхню столу.

В координатах кримінального права це має означати, що після того, як злочин вчинено, то вже не є можливим щось вдіяти для його зміни у той чи інший бік (наприклад, викреслити цю подію з загальної історії, перетворити його на інше менш значуще правопорушення без знесення змін у чинне законодавство, збільшити чи зменшити характер та(або) ступінь суспільної небезпеки вчиненого діяння тощо). Дійсно, з іншого боку, можливим є звільнення від покарання та його відбування (ст.ст. 74 – 87 КК України), або звільнення від самої кримінальної відповідальності (ст.ст. 44 – 49 КК України), в тому числі внаслідок певної посткримінальної поведінки (ч. 2 ст. 114, ч. 4 ст. 212 КК України). Але правова оцінка цих обставин значною мірою здійснюється окремо від оцінки самого правопорушення. Крім того, така правова оцінка відбувається саме у зв'язку з правопорушенням і без нього втрачає будь-який сенс. Незважаючи на можливі позитивні для суб'єкта злочину правові наслідки, об'єктивні характеристики правопорушення не змінюються, злочин не перестає бути злочином і не втрачає своєї суспільної небезпечності.

Між тим, з категоричністю твердження про лінійність та єдино можливий напрямок протікання часу погоджуються не всі. Так, Стівен Гокінг (Stephen William Hawking) [2, с. 89] не визнавав загальноприйнятий підхід щодо існування лише однієї послідовності розвитку подій у часі. Відкриття того, що швидкість світла виявилася однаковою для кожного спостерігача, незалежно від того, як він рухається, призвело до формулювання теорії відносності та відмови від ідеї про існування єдиного абсолютного часу. Замість цього кожен спостерігач одержав свою власну міру часу і це означає, що для різних спостерігачів час не обов'язково однаковий. Таким чином, час став більш особистим поняттям для спостерігача, який його вимірює. За теорією відносності, яка добре підтверджена численними експериментами, відсутнім є будь-який єдиний загальний вимір часу, з яким би погодились усі спостерігачі. Адже у кожного наявний свій власний вимір.

На переконання Стівена Гокінга, не слід розрізняти прямий і зворотний напрями часу, адже існують щонайменше три різних його стріли: 1) термодинамічна – напрям часу, в якому зростає безлад або ентропія; 2) психологічна – напрям, в якому ми відчуваємо плин часу, в якому ми пам'ятаємо минуле, але не майбутнє; 3) космологічна – напрям часу, в якому Всесвіт розширюється, а не стискається. При цьому умова безмежовості для Всесвіту разом із слабким антропним принципом не може пояснити, чому всі три стріли вказують в одному і тому напрямку, точніше, чому чітко визначена стріла часу має взагалі існувати. Якщо психологічна стріла визначається термодинамічною стрілою часу і вони обидві обов'язково завжди розгортаються в одному напрямку, то завдяки припущенню про безмежовість Всесвіту чітко визначені термодинамічна та космологічна стріли часу не будуть завжди вказувати в один і той самий бік впродовж всієї його історії.

Примітним є той факт, що несподівано для правників, з одного боку, та дослідників в галузі фізики або математики, з іншого боку, приклади зміни напрямку вектору часу, або впливу майбутнього на минуле, можливо відшукати у кримінальному праві, як за допомогою вищенаведеного прикладу, так і через наявність численних наступних.

У площині кримінального права спостерігачем світової лінії злочину може бути його суб'єкт, стороння особа, потерпілий або працівник правоохоронного органу тощо. Такі спостерігачі є втягнутими у коловорот подій з різним ступенем власної залученості, активності або пасивності. Виконавець злочину активно (дія) або пасивно (бездіяльність) сприяє тому, що відбувається. Не останньою мірою завдяки його конкретній поведінці певні події розгортаються у часі і просторі. Для подальшого дослідження розвитку

світової лінії злочину та ролі кожного з окреслених учасників в ній слід пригадати загально відомий у фізиці феномен впливу спостерігача на результати свого експерименту: якщо досліджують фотон світла як хвилю, він поводить себе як хвиля, якщо його досліджують як частку матерії, він поводить себе як частка матерії.

Чи може статися така ситуація, за якої працівник правоохоронного органу, що спостерігає за подіями, буде переконаний, що злочин є закінченим, принаймні, в його системі координат, але сам порушник ще матиме можливість впливати на ситуацію зі своєї власної системи координат? Позаяк не існує єдиного стандарту часу, а всі спостерігачі мають свій власний час, то на умовному годиннику прикордонника злочин виглядатиме вже закінченим, між тим як на умовному годиннику порушника він ще триває. Така інтерпретація виглядає провокативною тільки на перший погляд.

Так, моментом закінчення контрабанди (ст.ст. 201, 305 КК України) вважається момент перетинання суб'єктом злочину митного кордону України. Відповідно до положень ст. 10 Митного кодексу України митний кордон України збігається з державним кордоном України (крім деяких виключень, зокрема, меж штучних островів, установок і споруд, створених у виключній морській економічній зоні України, на які поширюється виключна юрисдикція України і які у межах цього дослідження можливо не враховувати). Таким чином, перетинання державного кордону буде означати одночасно перетинання митного кордону. Після перетинання державно-митного кордону, тобто, вже на території України, у відповідних підрозділів прикордонної та митної служби з'являються повноваження на виконання покладених на них функцій.

Для зручності роботи цих служб на практиці (у межах контрольно-пропускного пункту) вони територіально дещо розведені на відстань декількох метрів між собою і виконують свої завдання не одночасно (паралельно) по відношенню до конкретної особи, але послідовно. Як правило, особа спочатку спілкується з представниками прикордонної служби і далі проходить до пункту митної служби. У проміжку між ними вона може позбутися певних речей, наприклад, витягти з кишені пакунок з наркотичними засобами та відкинути його від себе. Якщо вона цього не зробить, то в момент зустрічі з митною службою у особи теж існує декілька варіантів поведінки у відповідь на традиційне в описаній обстановці запитання: 1) повідомити про те, що вона забула завчасно позбавитися незначної кількості речовини канабісу ще в Амстердамі (або іншому місці, звідки вона прибула і де її обіг не утворює складу кримінального або іншого правопорушення), але щойно пригадала та добровільно повідомляє про це представникам держави та віддає їм зазначену речовину, наслідком чого буде складання протоколу про адміністративне правопорушення; 2) приховати факт наявності речовини і бути викритою, наслідком чого буде притягнення до кримінальної відповідальності.

Між тим, у другому випадку таємний спосіб переміщення, як обов'язкова ознака об'єктивної сторони кримінального правопорушення за ст. 305 КК України, фактично буде реалізований вже після того, як відбулося переміщення речовини через державний (митний) кордон України. Тобто, після того, як спочатку мав місце процес переміщення (динаміка подій) та настав результат переміщення (статика, наслідок) і злочин в класичному розумінні вважається закінченим. Таким чином, кожна з форм незаконного переміщення (поза митним контролем або з приховуванням від митного контролю) повисає у повітрі, точніше – у часі, і є нереалізованою.

У цей незначний проміжок часу та на певному майданчику простору (відстані між постами прикордонників та митників) майбутній вибір поведінки, а саме, вибір певного способу поведіння (викрити себе або приховати певні обставини) буде впливати на

минуле (чи то було вже вчинено кримінальне, або адміністративне правопорушення, поки що є невідомим).

Якщо специфічною властивістю часу є його незворотність, тобто неможливість повернення в минуле, то дії особи у майбутньому (свідомий вибір варіанту поведінки під час спілкування з митною службою) не повинні впливати на минуле (фактичне перетинання державно-митного кордону як момент закінчення правопорушення). Але чомусь спосіб, що є обов'язковою ознакою об'єктивної сторони злочину контрабанда, все ж таки впливає на стан подій та їх правову оцінку вже після того, як правопорушення формально може вважатися завершеним.

Для кримінального права це відкриває простори захоплюючих світів Стівена Гокінга та інших рішучих дослідників, де час за певних умов може спливати з майбутнього через теперішнє у минуле.

І цей приклад з контрабандою теж не є поодиноким у кримінальному праві. Відсутні підстави розглядати його в якості аномалії або виключення. Так, відповідно до положень абз. 3 п. 24 постанови ПВСУ “Про судову практику у справах про злочини проти власності” від 06.11.09 р. № 10, якщо група осіб за попередньою змовою мала намір вчинити крадіжку чи грабіж, а один з її учасників застосував або погрожував застосуванням насильства, небезпечного для життя чи здоров'я потерпілого, то дії цього учасника належить кваліфікувати як розбій, а дії інших осіб – відповідно як крадіжку чи грабіж за умови, що вони безпосередньо не сприяли застосуванню насильства або не скористалися ним для заволодіння майном потерпілого.

В ситуації, коли особа у межах попередньої домовленості про вчинення крадіжки спостерігала за навколишньою обстановкою на вулиці, у житло не проникала, під час переростання крадіжки до розбою про потерпілих і поводження з ними не відала та насильства не застосовувала, а так само не сприяла його застосуванню, але надалі разом з іншими співучасниками зникла з місця події та отримала належну їй частку здобутого майна, то на підставі положень абз. 3 п. 24 постанови ПВСУ “Про судову практику у справах про злочини проти власності” від 06.11.09 р. № 10 буде вважатися, що вона скористалася таким насильством для заволодіння майном потерпілого. Така особа фактично потрапляє у пастку часу та обставин, стає їх заручником та позбавляється правових підстав посилаючись на експес з боку інших співучасників.

У просторово-часовому континуумі послідовність розвитку описаних подій, тобто світова лінія, що описує унікальну подорож правопорушника (одночасно й актора – активного учасника, і спостерігача експерименту під назвою життя) через чотирьохвимірний просторово-часовий континуум, буде виглядати наступним чином: особа виконує свою частину попередньої домовленості і забезпечує безпеку іншим співучасникам на місці події, і вже після того, як злочин було закінчено (розбій – з моменту нападу, крадіжка або грабіж – з моменту заволодіння майном та початкової можливості розпорядитися ним), у майбутньому у неї теж виникають наступні варіанти поведінки (припустимо, що у всіх випадках суб'єкт кримінального правопорушення не має інформації про фактичне переростання одного злочину в інший), зокрема: 1) відмовитися від одержання майна з будь-яких підстав та причин (тоді він не скористається наслідками застосованого насильства); 2) погодитися на частку здобутого майна та одержати її за взаємною згодою. У другому випадку особа з точки зору правової доктрини фактично використовує для свого неправомірного збагачення те насильство, яке було раніше застосоване до потерпілого, і перетворюється у співучасника розбою, що закінчився у минулому без його участі. Зазначена подія, що описується формулою “...надалі скористалася таким насильством для заволодіння

майном потерпілого...” відбувається у майбутньому, тобто вже після того, як минуле у вигляді вчиненого злочину (заволодіння майном із застосуванням насильства) залишилося позаду і його, здається, не можливо ані змінити, ані повернути.

Наведена правова кваліфікація, запропонована згаданою постановою ПВСУ від 06.11.09 р. № 10, є усталеною на практиці і майже не викликає вагань та сумніву під час застосування. Поруч з іншими описаними ситуаціями (контрабандою за ст. 305 КК України або умисним ухиленням від сплати податків, зборів (обов’язкових платежів) – ст. 212 КК України) вона підтверджує можливість впливу майбутнього на минуле не тільки у квантовій фізиці та математиці, але й у галузі кримінального права. Але якщо це так, то завдяки міжгалузевій взаємодії подібні випадки мають місце й в інших правових сферах.

Спорідненим прикладом може виступати феномен зворотної дії закону про кримінальну відповідальність у часі (ст. 5 КК України), коли подія у майбутньому (набрання чинності законом, що скасовує злочинність діяння, пом’якшує кримінальну відповідальність або іншим чином поліпшує становище особи) впливає на минуле (вважається, що такий закон поширює свою дію на минуле, тобто нібито був навіть тоді, коли його фактично не було).

З розглядуваними прикладами не слід плутати дію заохочувальних норм Особливої частини КК України (наприклад, ч. 5 ст. 110-2, ч. 2 ст. 114, ч. 4 ст. 212, ч. 2 ст. 255, ч. 6 ст. 258 КК України тощо), коли особа все одно вважається такою, що вчинила злочин, який надалі нічого не змінює у своїй правовій природі, але суб’єкт звільняється від кримінальної відповідальності в силу інших підстав та обставин.

Але й з посткримінальною поведінкою теж не все так одноставно. Відповідно до положень ч. 1 ст. 69 КК України суд наділений правом призначити основне покарання, нижче від найнижчої межі, встановленої в санкції статті (санкції частини статті) Особливої частини цього Кодексу, або перейти до іншого, більш м’якого виду основного покарання, не зазначеного в санкції статті (санкції частини статті) Особливої частини цього Кодексу за цей злочин. Умовами для цього є наявність кількох обставин, що пом’якшують покарання та істотно знижують (при цьому цікавим є питання, на який саме момент знижують – на час вчинення, або у майбутньому) ступінь тяжкості вчиненого злочину, а так само певна характеристика особи винного. Згідно з інформацією з Єдиного державного реєстру судових рішень, на практиці суди мотивують свою правову позицію щодо застосування положень ст. 69 КК України щирим каяттям та(або) визнанням вини, сприянням у розкритті злочину, повним або частковим відшкодуванням заподіяної шкоди, відсутністю судимості, позитивною характеристикою обвинуваченої особи, наявністю осіб, за якими необхідно доглядати, похилим або молодим віком обвинуваченої особи, її поганим станом здоров’я, з’явленням із зізнанням, думкою потерпілої особи щодо необхідної міри покарання, відсутністю тяжких наслідків, клопотанням сільського сходу щодо міри покарання [1], правдивими свідченнями підсудного, отриманням обоюдних тілесних ушкоджень, тривалим перебуванням підсудного під вартою тощо. У більшості випадків суди визнавали ці обставини необхідними та достатніми для застосування ст. 69 КК України, не відокремлюючи при цьому, які саме з них знижують ступінь тяжкості вчиненого злочину. Якщо відкинути обставини, що характеризують особу (відсутність судимості, позитивна характеристика, поганий стан здоров’я), або ті, що від неї не залежать (думка потерпілої особи, тривале перебування під вартою та інші), то шляхом виключення слід визнати, що окрема поведінка у майбутньому (з’явлення із зізнанням, правдиві свідчення) розглядаються суддівським корпусом в якості обставин, які у майбутньому

впливають на минуле та змінюють характеристику суспільної небезпечності вчиненої поведінки. Втім, не виключається, що наведені приклади застосування ст. 69 КК України є лише хибною практикою, яка заважатиме чистоті дослідження про вплив майбутнього на минуле у кримінальному праві.

Не виключається, що ще одним прикладом досліджуваної проблематики є феномен звільнення від кримінальної відповідальності у зв'язку із зміною обстановки (ст. 48 КК України). Ті невиразні пояснення, що містяться в учбовій та науковій літературі з цього приводу, тільки додають певної таємничості та натякають на можливість впливу майбутнього на минуле, адже зміною обстановки не є ані пряма декриміналізація вчиненого діяння, ані опосередкована декриміналізація, що може бути наслідком зміни нормативно-правового акту, на який посилається бланкетна норма диспозиції статті Особливої частини КК України (наприклад, скасування обов'язкового податкового платежу в ПК України).

В ситуації зі ст.ст. 201, 212, 305 КК України та переростанням крадіжки у грабіж або розбій все виглядає навпаки: майбутнє у формі певних дій (згода скористатися наслідками злочину проти власності, що фактично дорівнює згоді скористатися минулим насильством, тобто приєднатися до нього, або самовикриття після перетинання державно-митного кордону, або досягнення податкового компромісу тощо) вказує, за аналогією з котом Шредингера\* та відповідною квантовою невизначеністю, що злочин або був, або ні. І ця невизначеність у минулому спирається і залежить від подій у майбутньому. Таким чином, підтверджується вищенаведене парадоксальне припущення: подія у майбутньому перекроїла час і простір таким чином, що вчиненого злочину ніколи не було.

### **Висновки.**

Отже, з усією очевидністю зафіксовано можливість зміни напрямку вектору часу від майбутнього до минулого в царині кримінального права, що жодною мірою не може залишатися у межах тільки однієї галузі і через це взаємозв'язок між ними має значення для інших.

Світова лінія об'єктивної сторони окремого злочину у межах понятійного апарату кримінального права може проявлятися як певний акт поведінки, вчинений у передбачений законом спосіб, з урахуванням місця, обстановки, часу, використаних знарядь та інших матеріальних об'єктів або обставин. Цей акт з неминучістю викликає за собою певний наслідок. З усіма своїми елементами він розгортається в часі як процес, що має власну динаміку, тобто початок і розвиток (процес подій), та статику у вигляді його закінчення – певного наслідку.

Положення ст. ст. 48, 69 КК України та деяких інших, а так само особливості конструкцій ст.ст. 201, 212, 305 КК України тощо, вказують на існування реальної можливості у майбутньому вплинути на злочин, який був вчинений у минулому, в тому числі через значний проміжок часу після його закінчення. З іншого боку, це може виявитися або недоліком нормотворення, або хибною практикою, або зайвий раз підкреслювати умовність всього того, що відбувається у царині права.

---

\* *Примітка.* Кіт Шредингера, що одночасно перебуває у двох станах (живий і мертвий) – герой відомого уявного експерименту у квантовій механіці австрійського фізика-теоретика Ервіна Шредингера (Erwin Schrödinger). Згідно з принципами квантової механіки кожна елементарна частинка рівночасно може перебувати в декількох станах. Тож і удаваний кіт Шредингера в умовах експерименту може бути живий і мертвий водночас, допоки хтось не відчинить коробку й не визначить живий кіт чи ні.

Стає очевидним, що у кримінальному праві ніколи не піддавався сумніву субстанціальний підхід (Демокрит, Ісаак Ньютон та інші), відповідно до якого простір і час є незалежними одне від одного, діють поруч з матерією та безвідносно до неї. Але час у системі права може змінювати свій напрямок. Є підстави, наслідуючи ідеї Платона, Аристотеля, Альберта Ейнштейна, Стівена Гокінга та багатьох інших, вважати, що матерія, простір та час утворюють власну систему взаємовідносин, отже, вони залежать від взаємного руху, час може бути багатовимірним так само, як і простір (тобто, може бути визначений за допомогою не однієї, а декількох величин). Це означитиме, що час в окремих випадках у праві може бути ізотропним, тобто рівноправним у всіх своїх можливих напрямках руху.

Лінійність розгортання в часі обов'язкових ознак об'єктивної сторони конкретного складу злочину має місце не у всіх випадках. Інші, крім діяння та наслідку, обов'язкові ознаки об'єктивної сторони певного кримінального правопорушення можуть продовжувати реалізовуватися у часі та просторі навіть після того, як з правової точки зору настав момент його закінчення.

Час у праві є реляційною категорією, що допускає залежність його властивостей від характеру взаємодії об'єктів, подій та відносин.

Час у системі права може змінювати свій напрямок. Майбутнє у праві може впливати на минуле. Інше парадоксальне пояснення полягає у наступному: певна передбачена чинним законодавством подія у майбутньому здатна перекроїти простір і час у минулому таким чином, що вчиненого злочину ніколи не було. У прикладі з ухиленням від сплати податків, зборів (обов'язкових платежів) подальша поведінка платника або податкового агента змінює час і простір таким чином, що завдяки події у майбутньому (досягнення податкового компромісу) стає очевидним, що фактично вчиненого злочину (ухилення від сплати) ніколи не було.

Але такий вплив не є подорожжю у часі, адже не виявлено можливості викривити простір-час таким чином, щоб відбулося поєднання двох віддалених точок простору в одну і утворення тим самим так званої червоточини (мосту Ейнштейна – Розена).

У наведених прикладах з контрабандою та переростанням крадіжки у грабіж або розбій, можливо, має місце незначне викривлення часу-простору у кримінальному праві, або більш чи менш тривала петля часу, в яку потрапляє особа (контрабандист, вартівий на сторожі вчинення викрадення чужого майна) до тих пір, поки не реалізуються всі обов'язкові ознаки об'єктивної сторони злочину. Принципова можливість таких викривлень часу-простору доведена експериментально та пояснюється ефектом Гендріка Казимира (Hendrik Brugt Gerhard Casimir), відповідно до якого квантова теорія дозволяє від'ємну густину енергії. Виходячи з відомих на сьогодні законів, повернутися у минуле можливо лише у тому випадку, якщо історія вже зафіксувала будь-яким чином таке повернення (наприклад, сталася незрозуміла для очевидців подія, яку на той час не змогли пояснити, але це як раз і була поява мандрівника з майбутнього). Можливість такого повернення продовжувала би доволі незручно для кримінального права та інших галузей розхитувати постулат про свободу волі людини, на якому базуються всі теорії юридичної відповідальності, адже поки що про таку свободу стверджується лише тому, що ми не можемо повною мірою передбачити наступну поведінку певної людини. Але ми також не маємо можливості передбачити наступну поведінку вірусу, який мутує, та багато чого іншого.

*Перспективи подальших досліджень.* Порушені питання та надана їм наша оцінка є дискусійними та відкритими для обговорення з огляду на їх актуальність та важливість для забезпечення подальшого розвитку права. Вважаємо, що вказані в роботі проблеми

та проведені наукові дослідження можуть мати значення для розвитку не лише кримінального, а й інших галузей права, проте практика їх застосування потребує подальшого дослідження.

### Використана література

1. Вирок Жидачівського районного суду Львівської області від 14 листопада 2013 р. у справі № 443/244/13-к, провадження № 1-кп/443/25/13. URL: <http://www.reyestr.court.gov.ua/review/36013007> (дата звернення 15.08.2019).

2. Гокінг Стівен. Коротка історія часу. Від Великого вибуху до чорних дір; пер. з англійської. Перекладено за виданням “A Brief History of Time: From Big Bang to Black Holes”, Bantam Books відповідно до угоди з автором за посередництва агентства Writers House. Київ: К.І.С., 2015. 119 с. С. 89.

3. Радутний О.Е. Взаємодія між викладачем та студентом в світлі Болонської системи освіти та з урахуванням сучасних уявлень про енергоінформаційний обмін між дослідником та об'єктом дослідження. *Проблеми законності: зб. наук. праць Академії правових наук України*; відп. ред. В.Я. Тацій. Харків: Нац. юрид. акад. України, 2010. Вип. 110. 263 с. С. 209-214.

~~~~~ \* \* \* ~~~~~

УДК 316.324.8

БРИЖКО В.М., доктор філософії (Ph.D.) з юридичних наук, с.н.с.ORCID: <https://orcid.org/0000-0002-3941-1013>.**ПИЛИПЧУК В.Г.**, доктор юридичних наук, професор,
член-кореспондент НАПрН України.

ПРИВАТНІСТЬ, КОНФІДЕНЦІЙНІСТЬ ТА БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ

Анотація. У статті розглядаються окремі проблеми стану та формування правових основ системи захисту персональних даних в умовах євроінтеграції України у контексті застосування поняття “приватність людини” як фактору, який визначає основу інформаційної безпеки демократичного суспільства. Формулюються окремі пропозиції в плані можливого вдосконалювання сучасного законодавства.

Ключові слова: приватність, захист та безпека персональних даних, кіберзлочинність.

Summary. The article deals with certain problems of the state and formation of the legal foundations of the personal data protection system in the conditions of European integration of Ukraine in the context of the application of the concept of “human privacy” as a factor that determines the basis of information security of a democratic society. Proposals are formulated in terms of possible improvement of current legislation.

Keywords: privacy, protection and security of personal data, cybercrime.

Аннотация. В статье рассматриваются отдельные проблемы состояния и формирования правовых основ системы защиты персональных данных в условиях евроинтеграции Украины и в контексте применения понятия “приватность человека” как фактора, который определяет основу информационной безопасности демократического общества. Формулируются отдельные предложения в плане возможного совершенствования современного законодательства.

Ключевые слова: приватность, защита и безопасность персональных данных, киберпреступность.

Постановка проблеми. Необхідність створення умов захисту людини в контексті використання її персональних даних іншими людьми та суб'єктами влади з правового погляду досліджувалася та визначалася протягом значного історичного часу. Це пов'язано з поступовим і доволі тривалим становленням конституційних прав людини та спрямованості на формування правових засад недоторканності приватного життя.

Важливим при цьому є те, що особиста свобода невід'ємна від небезпеки. І справа по обмеженню свободи, з одного боку, є справою зміцнення безпеки людини, а з іншого – визначається потребами національної безпеки держави. Захист, хочемо ми цього чи ні, це обмеження, встановлені законом. Обмеження з боку правової держави мають сенс лише тоді, коли цими обмеженнями переслідується мета поставити перешкоди на шляху довільного поведіння з правами людини.

Метою статті є узагальнення проблемних питань приватності, конфіденційності та безпеки персональних даних, а також визначення логічності зв'язків між ними.

Виклад основного матеріалу.

Приватність та інформаційна приватність. Життя, бажання, мрії та діяльність людини завжди пов'язані зі словосполученням “недоторканність особистого життя”, еквівалент у застосуванні якого використовують у законодавстві США, англomовних країнах, публічних виданнях Європи та визначають терміном “*privacy*”. Цей термін є

запозиченням з латинської мови слова “*privaus*” – “приватний”, “особистий” та трактується як: особистість, інтимність, таємність, самотність, власність, між особисті відносини [1].

Узгодженого уявлення та юридичного визначення поняття “*privacy*” немає. Зустрічаються його різні розуміння та тлумачення, зокрема: “особисте життя, право на приватне життя, недоторканність приватного життя, право на самоту” [2].

В українській “Юридичної енциклопедії” “*privacy*” (укр. “прайвесі”) визначено як “приватна справа, таємниця, усамітненість” – правова категорія в англо-саксонській правовій системі, пов’язана із захистом інтимного життя людини [3].

В “Великому юридичному словнику” термін “*privacy*” тлумачиться як: “таємниця, самота, приватне життя” – особлива правова категорія, яка означає таємницю й недоторканність приватного життя, інтимну сферу людини. Термін може означати в одних випадках приватне життя, в інших – право на приватне життя, по-третє – право на захист недоторканності приватного життя і т.д.” [4].

У 1990 році, у Звіті Комітету Британії по конфіденційності та суміжних питань, було зазначено, що за результатами проведених досліджень трактувань “*privacy*” в рамках різних епох, культур та політичних систем “ніде не знайдено абсолютно прийнятного правового визначення цього поняття” [5].

Як вважається, історія *приватності* та безпосередньо пов’язаною з нею *конфіденційністю інформації* має більш як 3000 років, а у тому розумінні у якому її намагаються зрозуміти сьогодні – усього лише понад 150 років. Вона свідчить, що приватність раніше завжди була другорядною. На практиці потреба у виживанні часто затьмарювала бажання усамітнення. Не було класично-середньовічного латинського слова, еквівалентного “приватності”; було “*privatio*”, що визначалось як “відняти” [6].

Одне із тлумачень “*privacy*”, що часто використовується сьогодні, таке: приватність – це “право бути наданим самому собі”. Кожна людина має право на свій “куточок” у просторі, захищений від довільних зазіхань із боку [7].

Про “право бути наданим самому собі” вперше заговорили з 15 грудня 1890 року, коли американські юристи Луїс Брэндейс і Сэмюэль Уоррен опублікували в юридичному журналі Гарварда “*Harvard Law Review*” статтю “Право на приватність”. Вони писали, зокрема, що: “Інтенсивність і складність життя, пов’язані з розвитком цивілізації, сформували необхідність у самоті, і люди, під впливом культури, стали більш чутливим до публічності, через що самота й конфіденційність стали більш важливими для індивідуума; але сучасні підприємства й винаходи, вторгаючись в особисте життя людини, піддають його щиросердечному болю й стражданню, набагато більшим, ніж могли б заподіяти йому тілесні ушкодження” [8]. У подальшому, у 1928 р., суддя Луїс Брэндейс, який був вже членом Верховного суду США, стверджував що право на недоторканність приватного життя не можна ставити у залежність від способу, яким здійснюється отримання інформації про людину. Важливо не те, як технологічно або технічно здійснюється знімання інформації (зокрема, прослуховування), а те, що людина має право розраховувати на таємницю спілкування. Вказані думки формувались у часи, коли слів інформатизація, телекомунікації, Інтернет, штучний інтелект тощо взагалі не існувало, і мова йшла лише про “особисту недоторканість” у звичайній, не віртуальній, життєдіяльності. Й хоча батько права на приватність Луїс Брэндейс випередив свій час, тоді його стаття та погляди не одержали великого поширення, а те висвітлення, яке мало місце в пресі, не було харцизьким та не дуже притягало до себе уваги.

Проте, у 1934 р. “право бути наданим самому собі” було узаконено Рішенням Конгресу США та увійшло до складу основних джерел права, які існують у англо-саксонській системі прецедентного права. Поштовхом цьому слугував, як вважаємо, розвиток технологій індустріалізації й, що важливо для розуміння процесів щодо нашого часу стосовно інформатизації, на тій же підставі, на якій вона зараз актуалізується: вторгнення вже новітніх технологій (раніше це стосувалося комерції з комплектування картотек щодо збирання та продажу адрес, відомостей ПІБ, переписки з поштових карток, телефону, відомостей з медичних книжок та ін.) в особисте життя й несанкціонований та комерційний продаж інформації про людину.

З правової точки, можливо, більш-менш точний сенс “privacy” – це *право на недоторканність приватного життя*, тобто “право на себе”, що спрямовано на можливість людини “бути залишеною у спокої”. Хоча зрозуміло, що такі визначення прийнятно для англо-саксонській прецедентної правовій системи, але занадто широкі для застосування у романо-германської системі щодо предметно-нормативної практики, так як не визначають сутність ознак предметного захисту та не відповідають на питання – що для людини становить його втрата. Останнє важливо тому, що втрата або погіршення недоторканності приватного життя створює умови іншим здійснювати надмірну владу над психологічним, соціальним, економічним благополуччям та здоров’ям людини.

Сьогодні, в контексте уявлень про “privacy”, недоторканність приватного життя захищається ст. 12 Загальної декларації прав людини 1948 р., ст. 8, 12 Європейської Конвенції з прав людини та основоположних свобод 1950 р. та ст. 6-8, 11 Хартії основних прав Європейського Союзу 2000 р. та ін. міжнародно-правовими актами. Рішення Європейського Суду з прав людини постійно уточнюють сенс окремих формулювань.

Складовими приватного життя, що розглядалися з 1992 р. згідно із прецедентним правом у різних справах Європейського Суду із прав людини, є [9]:

- персональна ідентифікація. Визначалося, що це стосується зміни прізвища, реєстрації імен, а також зміни статі й внесення виправлень в акти цивільного стану;
- визначення законних зв’язків. Вказувалося, що важливою складовою приватного життя є доступ людини до інформації про своє минуле й свої родинні зв’язки, можливість не тільки встановлення, але й заперечування батьківства;
- фізична й моральна недоторканність. Визначалося, що обов’язкові медичні обстеження, примус до медичного й психіатричного лікування, фізичне насильство й відсутність юридичної можливості притягати винних до відповідальності, а також заборона на добровільну смерть і на аборт за медичними показниками можуть бути визнані втручанням у приватне життя;
- особистий простір. Розглядалися справи щодо “екологічних” прав людини, а також про публікацію світлин як інформації особистого змісту;
- збір і використання інформації. Визначалося, що сучасне суспільство неможливо уявити без систем спостереження, дактилоскопії, баз ДНК, офіційного перепису населення – уся зібрана в такий спосіб інформація, безумовно, стосується приватного життя;
- доступ до персональних даних. Мало місце рішення – незважаючи на те, що певна інформація може підлягати зберіганню, це не обов’язково означає, що особа, про яку вона зібрана, буде мати автоматичний доступ до неї;
- сексуальні відносини. Було рішення, що сексуальне життя окремої особи є частиною й важливим аспектом її особистого життя. Також заявники в Європейському Суді відстоювали своє право на гомосексуальні відносини, садомазохістську практику й публічну демонстрацію сексуальної поведінки;

- соціальна активність. Стосувалося можливості ефективної взаємодії з іншими людьми;
- професійні взаємини. На думку Суду, немає принципових підстав вважати, що поняття “приватного життя” виключає діяльність професійного та ділового змісту, саме у своїй роботі більшість людей мають значну, якщо не найбільшу, кількість шансів будувати відносини із зовнішнім світом.

Європейський Суд з прав людини також здійснив роботу з визначення недоторканності особистої переписки згідно ст. 8 Європейської Конвенції з прав людини та свобод 1950 р. Важливим є те, що Суд уточнив обставини, за яких державі дозволено порушити цю недоторканність, а також виробив стандарти перехоплення телефонних повідомлень (розмов), які підлягали захисту згідно з Конвенцією як “кореспонденція”. Щоб перехоплення не було порушенням, воно має здійснюватися [10]:

1. *“На підставі закону”*. Будь-яке спостереження має проводитися згідно національного закону, що має задовольняти наступні вимоги:

- доступність – громадянин повинен мати можливість переконатися, що прослуховування відповідає нормам закону;
- передбачуваність – громадянин повинен бути здатний (при необхідності за допомогою адвоката) передбачити наслідки будь-якої можливої дії;
- якість – закон повинен мати ефективні заходи проти можливих зловживань.

Зокрема, це означає, що закон має визначати:

- список злочинів, здійснення яких може призвести до прослуховування;
- обмежуватися випадками, коли фактичні підстави підозрювати особу в здійсненні тяжкого злочину вже виявлені іншими засобами;
- санкціонувати прослуховування тільки на підставі мотивованої письмової заяви високої посадової особи;
- дозволяти прослуховування тільки після одержання санкції органа або посадової особи, що не належить до виконавчої влади (судді);
- установлювати обмеження на тривалість прослуховування, із вказівкою періоду часу;
- визначати правила складання звітів щодо змісту прослуховування;
- обмежувати обмін матеріалами прослуховування між державними органами;
- визначати обставини, за яких записи прослуховування слід знищити;
- ухвалити рішення, що робити з матеріалами прослуховування, якщо обвинувачувану особу (жертву) буде виправдано. Будь-яка особа в країні, де діють положення про таємне прослуховування, може вимагати визнання себе жертвою без будь-якого обов’язку надавати докази про те, що спостереження дійсно велось.

2. *“Як необхідність у демократичному суспільстві”*. Прослуховування має бути:

- тільки такою мірою, яка необхідна для безпеки демократичних інститутів;
- за виняткових умов та в інтересах національної безпеки й/або попередження безладу або злочинів.

На думку закордонних спеціалістів, юридичне забезпечення права на приватність означає встановлення й дотримання меж припустимого втручання в будь-яке приватне життя, що виходить із таких наступних посилок [11]:

- границі між публічною і приватною сферами інтересів, в останню з яких інші люди, організації й або уряди не можуть вторгатися (також стосується обліку біометричних даних як еквіваленту тіла людини);
- форми діяльності, поведінки й способу дій, які людина має право захищати (приховувати) від уваги сторонніх;

- захист від вторгнення в приватне життя й свобода вибору його форми;
- можливістю людини контролювати інформацію про себе – вирішувати, коли, як і в якому обсязі інформація про неї стає відомою або повідомляється іншим.

Сьогодні приватність розглядається як фундаментальне право людини й перебуває в одному ряді із правом на життя, свободою переконань, власністю на майно та особисті здобутки на результати інформаційної та інтелектуальної праці.

Фахівці громадських організацій, Electronic Privacy Information Center та Privacy International, у своєму спільному дослідженні запропонували (умовно) розділити приватність на чотири види [7]. Це:

- фізична приватність – це умови захисту від примусових для людини процедур, зокрема медичних та багато ін. Деякі міри обумовлені потребами врахування інтересів суспільства та держави. Так поліції надане право зняти в арештованого відбитки пальців або узяти в нього аналіз ДНК для включення в національну базу даних і т.п.;

- територіальна та майнова приватність – звичайно мається на увазі недоторканність фізичних речей та житла. Певний рівень приватності мають не тільки будинки й квартири, але й робочі місця, готельні номери, купе поїзда і т.д. Майнова приватність визначається правом власності на майно та правом використання об'єктів інтелектуальної власності. Право власності на інформаційний продукт законодавством не визначається, хоча інформацією завжди торгували і вона знаходиться у комерційному у обігу;

- інформаційна приватність – під цим розуміється наявність захисту прав людини та свобод в інформаційній сфері, її уявлень та намагань покращити своє життя;

- приватність комунікацій – це все, що пов'язане з технічними засобами та техніко-технологічними діями, які стосуються, зокрема, таємниці телефонних розмов, поштових, електронних повідомлень. Приватність комунікацій найтіснішим чином пов'язана з інформаційною приватністю, зокрема з Інтернетом, який, як ніколи раніше, надає можливості несанкціонованих контролю та впливу на особисте життя людини.

Інформаційна приватність завжди займала особливе місце у стосунках між людьми. Її основою є забезпечення захисту відомостей про людину щодо нецільового та несанкціонованого отримання та використання її персональних даних.

Виділяють наступні елементи права на інформаційну приватність:

- право на самотність;
- право на інтимність;
- право на анонімність;
- право контролювати інформацію про себе [9], а також
- право “бути забутим” [12, с. 40].

У законодавстві це передбачає наявність пріоритетних гарантій забезпечення умов приватності для будь-яких дій по відношенню до персональних даних, які повинні:

- бути отримані законним способом;
- збиратися з відома й згоди особи, у кількості мінімально необхідній для певної мети;
- бути точними й захищеними від несанкціонованого доступу;
- використовуватися тільки з метою, заради якої вони були отримані;
- надаватися третім особам тільки за згодою особи, про яку вони зібрані;
- бути доступними тій особі, якої вони стосуються, зокрема, в контексті права на одержання інформації про її використання з виправленням невірної інформації та права доступу до комп'ютерних даних;
- знищуватися після того, як мета, заради якої їх збирали, досягнута й у даних більше немає потреби.

Зазначені гарантії не є абсолютними, а значною мірою залежать від контексту, у рамках якого визначаються норми захисту приватного життя й вимоги того, що може й повинне бути розкрито для публічності або держави [11]. Тобто, вважається, що границі інформаційної приватності рухливі й засновані на бажанні або небажанні індивіда повідомляти ту або іншу інформацію про себе.

Слід також звернути увагу на те, що визначення приватності людини в термінах права на контроль використання інформації про себе – одна з основних тенденцій за кордоном в політичних і юридичних дискусіях про захист персональних даних [13].

Сьогодні забезпечення інформаційної приватності дедалі більше ускладнюється у зв'язку з поширенням телекомунікаційних технологій та мереж. Вже загально зрозуміло, що будь-які відомості про людину можуть бути отримані завдяки Інтернет-технологіям та використані не лише на її користь, а з метою маніпулювання свідомістю, вимагання грошей, шантажу, залякування, або, нерідко, щоб проштовхувати на ринок якийсь комерційний продукт та ін. Зазначені дії безпосередньо стосуються проблеми забезпечення безпеки інформаційної приватності персональних даних в Україні, яка є невід'ємною складовою забезпечення національної безпеки держави.

Разом з вказаним зазначимо, що в українському законодавстві немає та не використовується поняття “приватність” за виключенням її згадування у ст. 182 КПК України та у нормативному документі КМ України – “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108. Стаття 8 “Захист персональних даних” Угоди визначає: *“Сторони зобов’язуються вживати необхідних заходів відповідно до національного законодавства у сфері охорони приватних персональних даних з метою захисту персональних даних українських громадян, відібраних для тимчасового працевлаштування відповідно до цієї Угоди, у тому числі від випадкової їх втрати, пошкодження, незаконної обробки та доступу”* [14].

Конфіденційність персональних даних в Україні. Згідно ст. 10 Закону України “Про інформацію” (2016 р.) одним з видів інформації за змістом є те що вкладається в поняття “відомості про фізичну особу” або “персональні дані людини”. Вони є складовою та невід'ємною частиною будь-яких професійних таємниць.

Сьогодні існують багато видів професійних таємниць, у основі яких лежить так звана “конфіденційність” інформації (confidentia – від англ. “довіра”). Вона, згідно ст. 21 Закону України “Про інформацію” (2016 р.), у функціональному колі свого предмета призначення передбачає наявність забезпечення захисту персональних даних у конфіденційному порядку, зокрема в таких сферах діяльності, як комерційна, податкова, банківська, адвокатська, нотаріальна, журналістська тощо, навіть у таємниці сповіді. Однак, проблема у тому, що дефініції, тобто наявності визначення істотних ознак предмета поняття під назвою “конфіденційна інформація”, у законі 2016 р. немає. Її було вилучено з однойменного Закону України 1992 р. Стосовно сфери інформаційно-комунікаційної приватності в українській юридичній енциклопедії також маємо твердження про те, що персональні дані є конфіденційною інформацією [20].

Сучасне законодавство України має значну кількість законів, які надають лише переліки інформації про особу з посиланням на її “конфіденційність”, без нормативного визначення (дефініції) та легального (предметно-правового) застосування словосполучення “конфіденційна інформація”, як це прийнято у романо-германської (континентальної) системі права, яка притаманна і Україні. Наведемо деякі з них:

Конституція України від 28.06.96 р. № 254к/96-ВР (ст. 32) – ...не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. *Примітка.* Слово “приватність” у Конституції не використовується.

Цивільний кодекс України від 28.02.19 р. № 2694-VIII (ст. 895) – визначає конфіденційними – відомості щодо предмета договору на виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, хід їх виконання та результати. *Примітка.* Самого визначення поняття “конфіденційність” немає.

Кримінальний кодекс України від 06.06.19 р. № 2747-VIII (ст. 182) – має лише одне згадування про конфіденційність: порушенням недоторканності приватного життя є незаконне збирання, зберігання, використання, знищення, поширення конфіденційної інформації про особу або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями Кодексу. *Примітка.* Визначення поняття “конфіденційність” відсутнє.

Податковий кодекс України від 07.12.17 р. № 2245-VIII (п. 70.15) – до конфіденційної відноситься інформація про реєстраційний, ідентифікаційний номер платника податків, номер облікової картки фізичної особи тощо. *Примітка.* Словосполучення “конфіденційна інформація” застосовано у ст. 17.1.9 – платник податків має право: на нерозголошення контролюючим органом (посадовими особами) відомостей про такого платника без його письмової згоди та відомостей, що становлять конфіденційну інформацію, державну, комерційну чи банківську таємницю та стали відомі під час виконання посадовими особами службових обов’язків, крім випадків, коли це прямо передбачено законами. Визначення поняття “конфіденційність” відсутнє.

Митний кодекс України від 19.12.19 р. № 395-IX (ст. 11) – про додержання вимог щодо конфіденційності інформації; (ст. 37) – використовує словосполучення “інформація конфіденційного характеру”. *Примітка.* У суспільних відносинах, тобто у юриспруденції (а не у публіцистиці), ніяка інформація, відомості або дані не мають характеру; характер – це психічні, моральні та інтелектуальні складові здібності лише біологічної істоти. Визначення поняття “конфіденційність” відсутнє.

Закон України “Про інформацію” від 06.12.16 р. № 1774-VIII (ст. 11) – до конфіденційної інформації про фізичну особу (персональні дані) належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров’я, а також адреса, дата і місце народження. *Примітка.* У техніці складання нормативних формул звичайно уникають її незавершеності (стосується слова “зокрема”). Визначення поняття що таке “конфіденційність” не маємо, мова йде лише про окремі її види.

Закон України “Про доступ до публічної інформації” від 09.04.15 р. № 319-VIII (ст. 7) – конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб’єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов. *Примітка.* Ця дефініція визначає процес надання доступу, але не надає визначення про сенс та предметно-правовий зміст поняття “конфіденційна інформація”.

Закон України “Про друковані засоби масової інформації (пресу) в Україні” від 02.10.18 р. № 2581-VIII (ст. 2) – має лише згадування наявності “конфіденційності” в контексті свободи діяльності друкованих засобів масової інформації.

Закон України “Про телебачення і радіомовлення” від 02.10.18 р. № 2581-VIII (с. 56.) – має лише згадування в контексті вимог до розповсюдження конфіденційної інформації. Крім цього, без згадування конфіденційності (ч. 3 ст. 62) – у програмах та передачах телерадіоорганізації не мають права без письмової згоди батьків або осіб, що їх

замінюють, а також відповідних правоохоронних органів розголошувати будь-яку інформацію, яка може сприяти ідентифікації особи неповнолітнього правопорушника або яка стосується факту самогубства неповнолітнього.

Й далі, в контексті визначення конфіденційності приватних (особистих) відомостей (інформації, даних) в інформаційно-комунікаційній сфері, де предметно-понятійного визначення поняття “конфіденційність” не маємо.

Закон України “Про свободу пересування та вільний вибір проживання в Україні” (ст. 6 ч. 8.) – відомості про місце проживання.

Закон України “Про загальнообов’язкове державне соціальне страхування у зв’язку з тимчасовою втратою працездатності та витратами, зумовленими похованням” (ст. 33) – відомості про страховий стаж, результати медичних обстежень, отримані доходи застрахованої фізичної особи.

Закон України “Про звернення громадян” (ст. 10.) – відомості про особисте життя громадян, одержані із звернень громадян.

Закон України “Про загальнообов’язкове державне пенсійне страхування” (ч. 1. ст. 98) – інформація про стан пенсійних активів, облікованих на накопичувальному пенсійному рахунку застрахованої особи.

Закон України “Про недержавне пенсійне страхування” (ст. 53 ч. 3.) – інформація про пенсійні внески, пенсійні виплати та інвестиційний прибуток (збиток), що обліковується на індивідуальному пенсійному рахунку учасника пенсійного фонду, пенсійні депозитні рахунки фізичних осіб, договори страхування довічної пенсії;

Закон України “Про оплату праці” (ст. 31) – відомості про оплату праці працівника.

Закон України “Про лікарські засоби” (ст. 9 ч. 8.) – інформація, що міститься в заяві про державну реєстрацію лікарського засобу та додатка до них.

Закон України “Про біженців та осіб, які потребують додаткового або тимчасового захисту” (ст. 7 ч. 10) – відомості, що подаються заявником на визнання біженцем або особою, яка потребує додаткового захисту.

Закон України “Про забезпечення безпеки осіб, які беруть участь у кримінальному судочинстві” (ст. 15) – дані про особу взятую під захист у кримінальному судочинстві.

Закон України “Про державний захист працівників суду і правоохоронних органів” (ст. 10) – дані про працівника суду або правоохоронного органу, взятого під захист.

Закон України “Про доступ до судових рішень” (ст. 7) – відомості, що містяться в текстах судових рішень та дають можливість ідентифікувати фізичну особу, зокрема: імена (ім’я, по батькові, прізвище) фізичних осіб; місце проживання або перебування фізичних осіб із зазначенням адреси, номерів телефонів чи інших засобів зв’язку, адреси електронної пошти, ідентифікаційних номерів (коди); реєстраційні номери транспорту.

Закон України “Про Всеукраїнський перепис населення” (ст. 16) – первинні дані, отримані в процесі проведення Перепису населення.

Закон України “Про поховання та похоронну справу” (ст. 7) – інформація про померлого, та багато ін. нормативних актів.

За підсумками можна сказати, що українське законодавство загальносистемного визначення поняття “конфіденційність” не має та не застосовує. Існуючий підхід до захисту персональних даних в Україні йде по шляху, на якому відсутні загальні юридичні критерії поняття “конфіденційна інформація” яка має особливі властивості, що обумовлюють потребу в конкретних умовах дотримання її приватності в використанні та у відповідних засобах захищеності, і не вирішене питання місця персональних даних у обсязі відповідності логічному колу цього поняття.

До зазначеного вважаємо за необхідне звернути увагу на те, що згідно п. 4.1.1.2 існуючого в Україні з 1997 року нормативного акту – ДСТУ 3396.2-97 “Технічний захист інформації. Терміни та визначення” [21]: *“конфіденційна інформація – це інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними”*. При цьому, у п. 2 Передмови до Стандарту визначено, що його вимоги забезпечують реалізацію норм Закону України “Про інформацію”. Але, як зазначалося раніше, ця нормо-дефініція (тобто, стаття 30) з Закону було вилучено у 2011 р. До слова, з Закону також було вилучено норми щодо “право власності на інформацію” (ст. 38) та “визначення інформації товаром” (ст. 39), і взагалі він був перетворений у засіб забезпечення діяльності ЗМІ.

Головне полягає у тому, що наведена вище дефініція визначає триаду повноважень права власності людини, а саме: права володіння, користування і розпорядження своїми відомостями-даними, про що детально йдеться у [12, с. 90-97; 22, с. 163-175]. Саме ця дефініція є чіткою класифікацією критеріїв за якими визначається наявність предмету приватності та конфіденційності інформації для будь-якого виду персональних даних. І це важливо з погляду активного поширення процесів щодо електронно-інформаційного середовища, у якому традиційні нормативні підходи й організаційні механізми щодо захисту персональних даних свідчать про їхню малу ефективність.

Безпека приватності персональних даних. В українському законодавстві немає словосполучення “безпека приватності персональних даних” (або “безпека персональних даних”), закріплено лише термін “інформаційна безпека” у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки” від 09.01.07 р. № 537-V. Згідно п. 13 Розділу III Закону інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації. Про “процес” захищеності не йдеться.

Відповідно до Доктрини інформаційної безпеки України [15] до суттєвих ознак поняття “інформаційна безпека” віднесено:

- *конфіденційність* – стан поводження з інформацією, при якому доступ до неї отримують тільки суб’єкти, які мають на це право;
- *цілісність* – запобігання несанкціонованій або незаконній модифікації інформації;
- *доступність* – запобігання тимчасовому або постійному приховуванню інформації від користувачів, які мають право на доступ.

Виходячи, зокрема, з вищенаведеного, *безпеку приватності персональних даних вважаємо за необхідне розглядати не лише як стан захищеності відомостей про особу, а й процес забезпечення їх захисту.*

В наш час поширення інформаційно-віртуальної реальності, яка раніше лише проявлялася у житті, завдяки швидкому розвитку ІКТ, мереж поняття “приватності” та юридичного захисту персональних даних дедалі більше перетворюється на нормативно-фіктивну сферу намірів та бажань в упорядкуванні суспільних відносин, де усе більш складно уявити собі світ, у якому буде існувати приватність. Зростаючі збір, об’єднання та обробка персональних даних в різних базах, що документують деталі ідентифікаційних та фізичних атрибутів, поведінку, бажання, відносини, недоліки, досягнення та будь-що ін., створює таке уявлення про людину, коли можна вже вести розмову про наявність лише *віртуальної приватності з віртуальною конфіденційністю.*

Глобальні інформаційні мережі й безліч сервісів несанкціоноване та непомітно збирають про користувачів терабайти даних, та й самі користувачі постійно викладають своє життя на загальний огляд у соцмережах, з різних причин.

Так, до прикладу, коли користувачі Інтернету намагаються ввійти до якогось сайту або бази даних, вони натрапляють на обов'язкові для відповіді запитання. Потім їх електронні відповіді та е-сліди автоматизовано обробляються та поширюються з одного сервера на інший, фільтруються, сортуються, аналізуються, зберігаються у невідомих базах даних, хмарних сховищах (сервісів, які все ще мають високі ризики їхнього залучення) та використовуються з невідомою для суб'єкта даних ціллю. Звичайно відповіді “для чого” немає, проте мало хто хвилюється з цього приводу.

Тим часом нецільове використання персональних даних здатне завдати людині великої шкоди. Особливо якщо мова йде про “чутливі персональні дані” (sensitive personal data), які потребують особливо делікатного до них ставлення, тобто особливих заходів у законодавчому захисту, наприклад інформація про стан здоров'я. Відомі не тільки випадки, коли медичні діагнози проти бажання пацієнта розміщалися в мережі з баз даних лікувальних закладів, і наслідки виявлялися досить жалюгідними, а взагалі давно поширена практика, коли Інтернет використовують для пропозицій з продажу різноманітних баз персональних даних.

Сьогодні інформаційно-комп'ютерні технології є потужним інструментом для злочинців різних країн, який вони можуть використовувати для протиправної діяльності, у тому числі на транснаціональному рівні. Боротьба з кіберзлочинністю стає однією з головних тем сучасної міжнародної політики, де проглядаються намагання пошуку балансу між приватністю та безпекою. Найкраще це помітно на прикладі Європейської Конвенції про кіберзлочинність.

Робота над Конвенцією в Раді Європи почалася навесні 1997 року [16]. Це був закритий процес, у якому брали участь не тільки представники європейських держав, але і юристи Департаменту юстиції США. Через три роки, коли число версій дійшло до 22, публіка змогла познайомитися з текстом. На його творців посипалися гнівні листи. Уважалося, що Конвенція встановить європейські стандарти в боротьбі з атаками на комп'ютерні системи, шахрайством у мережі, поширенням вірусів, порнографії, пропагандою насильства й т.п., що зрозуміло. Інтернет не має границь, цим користуються злочинці. І виходить, як стверджували розробники Конвенції, настав час поставити “на безмежну основу” і роботу правоохоронних органів різних країн. Вони запевняли, що поки Конвенції немає, можливі будь-які порушення, а от якщо вона буде прийнята, процес боротьби зі злочинністю стане більш ефективним. Однак, розширивши повноваження спецслужб, було занадто мало приділено уваги гарантіям прав користувачів Інтернету.

18 жовтня 2000 року кілька десятків громадських організацій виступили із загальним відкритим листом проти Конвенції. Критикували, зокрема, ідею зобов'язати провайдерів Інтернету складати звіти про дії клієнтів. Автори відкритого листа вважали, що стаття 18 проекту несумісна зі статтею 8 Європейської Конвенції з прав людини й з рішеннями Європейського Суду. Схожі думки було від незалежних експертів, журналістів і деяких державних чиновників. Наприклад, Комісари з захисту персональних даних під час своєї зустрічі в Стокгольмі у квітні 2000 року висловили стурбованість проектом Конвенції. Проте 8 листопада 2001 року документ був схвалений Радою Європи.

Учасниками Конвенції є 35 європейських держав-членів Ради Європи та 5 держав, які не є членами Ради Європи (Австралія, Домініканська Республіка, Японія, Панама, США) [17]. Конвенція є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних

даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню та переслідуванню, як на внутрішньодержавному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Згідно з положеннями Конвенції, Сторони надають одна одній взаємну допомогу з метою розслідування або переслідування кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі.

Сторона може запитати іншу Сторону видати ордер чи іншим чином провести термінове збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території такої іншої Сторони, і відносно якої Сторона, яка запитує, має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу, арешту чи подібних дій або розголошення таких даних.

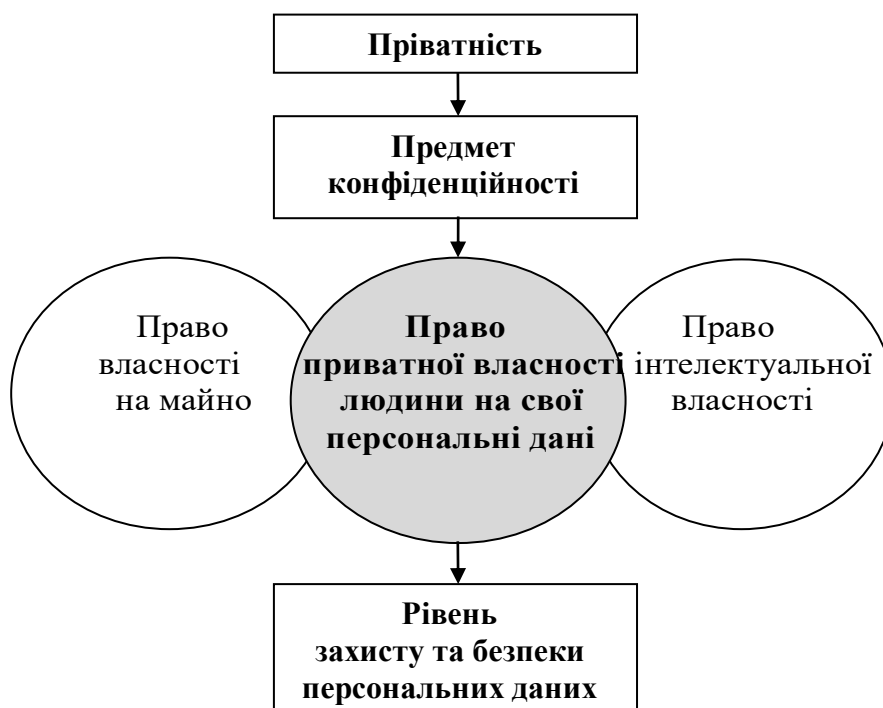
У 2011 році в ООН була створена Міждержавна група експертів з вивчення кіберзлочинності, зусиллями якої у 2013 році було проведено "Всебічне дослідження проблеми кіберзлочинності" [18]. У цьому документі проаналізовані такі аспекти як законодавство у даній сфері, діяльність правоохоронних органів, міжнародне співробітництво тощо. В ньому, зокрема, зазначається, що 80 відсотків кіберзлочинів вчиняється в організованій формі. Сьогодні Робота міждержавної групи експертів продовжується. Так у доповіді за наслідками засідання даної групи 27-29 березня 2019 року у Відні були розглянуті питання удосконалення законодавства, у тому числі міжнародного, проблеми діяльності правоохоронних органів, використання електронних доказів. Було зазначено, що, зважаючи на транснаціональний характер кіберзлочинності і той факт, що значна більшість глобальних кіберзлочинів вчиняються організованими групами, державам-членам слід більш широко застосовувати Конвенцію ООН проти транснаціональної організованої злочинності для сприяння обміну інформацією та доказами в ході кримінальних розслідувань, що стосуються кіберзлочинності.

В Україні Конвенція про кіберзлочинність 2001 року набула чинності 1 липня 2006 року [19]. Центральними органами України, які уповноважені розглядати відповідні запити компетентних органів іноземних держав, а також направляти запити до компетентних органів іноземних держав на підставі та на умовах, визначених Конвенцією, є Міністерство юстиції України (щодо виконання судових рішень) та Генеральна прокуратура України (щодо процесуальних дій під час розслідування кримінальних справ). Порядок і умови розгляду відповідних запитів компетентних органів іноземних держав, так само як і направлення запитів до компетентних органів іноземних держав, визначені Главою 42 Кримінального процесуального кодексу України. Відповідно до Закону України "Про внесення зміни до Закону України "Про ратифікацію Конвенції про кіберзлочинність" від 21.09.10 р. № 2532-VI в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [18].

Висновки.

1. Приватність та безпека персональних даних забезпечується нормативно-правовими умовами конфіденційності відомостей. Рівень конфіденційності, як стан та процес захисту приватності, впливає на загальне становище інформаційної безпеки в Україні.

У контексті наявності логічності взаємозв'язків (кореляції) приватності, конфіденційності та безпеки персональних даних вважаємо за можливе виходити з того, що вони проявляються у властивостях виду персональних даних у будь-якій області приватності (прайвеси), визначаються предметом інформаційної конфіденційності в обсязі права приватної власності людини на дані про себе, яке забезпечує захист та відповідний рівень безпеки персональних даних. Використовуючи раніше здійснені наробітки щодо визначення обсягу та зв'язку суттєвих ознак різних понять (“право власності на майно”, “право інтелектуальної власності” та “право приватної власності людини на свої персональні дані”), які, згідно логічних кругів Ейлера завжди частково збігаються (див. [12, с. 92-93]), взаємний зв'язок та співвідношення між приватністю, конфіденційністю, захистом та безпекою персональних даних наочно може бути подано таким чином:



2. Сучасне законодавство, зокрема в Україні, не має юридичного визначення таких понять, як “приватність” (privacy) та “безпека персональних даних”. Враховуючи дедалі активніше їх застосування у наші часи, вони потребують юридичного визначення, яке відображає істотні ознаки їх предметного змісту.

Те ж саме стосується поняття “конфіденційна інформація”, яка має особливі властивості, що обумовлюють потребу в конкретних умовах дотримання її приватності в використанні та у відповідних засобах захищеності. А це визначає необхідність запровадження чітких істотних ознак (критеріїв) щодо поняття “конфіденційність”.

У загальному плані вважаємо, що законодавству України потрібні не стільки переліки видів персональних даних, кожен з яких за різних уявлень може бути суб’єктивно віднесений (або не віднесений) до категорії “конфіденційність”, а практичне запровадження та застосування уніфікаційних критеріїв, які й визначають предмет конфіденційності, зокрема в сфері захисту персональних даних. Уніфікація надає системний підхід до конкретності у визначенні наявності інформаційно-комунікаційної приватності, особливо в умовах поширення застосування засобів електронно-інформаційного середовища, запобігає розпорошеності по законодавству

відомостей у численних наборах переліків, створює однаковість у підході до кваліфікації персональних даних конфіденційними, сприяє більш чіткій модальності суджень у побудові усієї системи захисту та безпеки персональних даних.

3. У сучасних умовах поширення ІКТ та мереж боротьба з кіберзлочинністю стає однією з головних тем сучасної міжнародної політики, де проглядаються намагання пошуку балансу між приватністю та безпекою. Баланс між приватністю та безпекою персональних даних – складне питання, яке в епоху інформатизації не може вирішуватися політиками, юристами, технічними фахівцями або спецслужбами на підставі поглядів минулого часу. Захист персональних даних взагалі не зводиться лише до вимог забезпечення якості технічної обробки даних і посилення заборонних заходів в інтересах створення умов загальної безпеки. Виходячи з приписів ст. 3 Конституції України, яка визначає наявність та пріоритетність природних прав людини, – *“Людина, її життя і здоров’я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави...”*, мірою оцінки суджень про допустимість втручання в особисте життя може стати “право приватної власності людини на свої персональні дані” та “контроль використання інформації про себе”, за умов правового обмеження у правах фізичних осіб, якщо це офіційно та чітко визначено, що стосується державної чи громадської безпеки, фінансової стабільності, боротьби зі злочинністю, захисту прав та основоположних свобод інших осіб.

Використана література

1. Прохвачева О. (2000) Лингвокультурный концепт “приватность”. URL: <http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM>
2. Большой англо-русский словарь; под ред. проф. И.Р. Гальперина. Москва, 1988 г.
3. Юридична енциклопедія: в 6 т.; редкол. Ю.С. Шемшученко (голова редкол.) та ін. Київ: “Українська енциклопедія”, 2003. Т. 5 : П–С. С. 53.
4. Большой юридический словарь; под ред. А.Я. Сухарева, В.Е. Крутских. Москва: Инфра-М, 2003.
5. Report of the Committee on Privacy and Related Matters. Responsibility: Chairmant David Calcutt. Cmnd. 1102. London: H.M.S.O., 1990; Особливості захисту персональних даних і сучасному кіберпросторі: правові та технологічні аспекти: анал. доповідь. Київ: Нац. інст. страт. досл., 2013. 51 с. С. 4.
6. Приватность: рождение и смерть. 3000 лет истории приватности. URL: <https://www.habr.com/ru/company/parallels/blog/348922>
7. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: [//www.epic.org](http://www.epic.org); Смирнов С. Приватность. Москва: Изд. “Права человека”. 2002. 95 с. С. 9.
8. Brandeis Louis D, Warren Samuel D. The Right to Privacy. *Harvard Law Review*. 1890. P. 193-220. URL: <https://www.louisville.edu/library/kaw/brandeis/privacy/html>
9. Соколова М. (2014). Защита персональных данных он-лайн: основные понятия. URL: https://www.researchgate.net/publication/281459597_Zasita_personalnyh_dannyh_onlajn_osnovnye_ponatia
10. Прослушивание телефонов в международном праве и законодательстве одиннадцати европейских стран: сост. Е. Захаров. – (Харьковская правозащитная группа). Харьков: Фолио. 1999. 152 с. С. 14-15.
11. Westin A. (2003) Social and Political Dimensions of Privacy. URL: <http://www.asc.upenn.edu/usr/ogandy/Gandy%20Comm664/westin%20-%20social%20and%20political%20dimensions%20of%20privacy.pdf>

12. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія; за ред. В.М. Брижка, В.Г. Пилипчука. – (НДІП НАПрН України). Київ: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с.

13. Bygrave L. (2010) Privacy and data protection in an international perspective. URL: <http://www.uio.no/studier/emner/jus/jus/JUS5630/v13/undervisningsmateriale/privacy-and-data-protection-in-international-perspective.pdf>

14. “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108. URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webpro c4 _1?pf3511=59911

15. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”: Указ Президента України від 25.02.17 р. № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>

16. Дембич Д.А. Обзор проекта Европейской конвенции о преступности в киберпространстве. URL: http://www.conf3.parkmedia.ru/any_r.asp?; Волеводз А.Г. Проект Европейской Конвенции о киберпреступности: особенности и новации правового регулирования международного сотрудничества в противодействии компьютерным преступлениям. *Защита информации. Конфидент*. 2001. № 5. С. 18-25, № 6. С. 23-27.

17. Сайт Мініюсту України. URL: <https://www.minjust.gov.ua/news/ministry/1-lipnya---vos ma-richnitsya-nabuttya-chinosti-dlya-ukraini-konventsii-pro-kiberzlochinnist-20026>

18. Гуцалюк М.В. Загрозливі тенденції організованої кіберзлочинності. *Інформація і право*. № 1(32)/2020. С. 88-98.

19. Конвенція про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575

20. Юридична енциклопедія: в 6 т.; редкол. Ю.С. Шемшученко (голова редкол.) та ін. Київ: “Українська енциклопедія”, 2001. Т. 3: К–М. С. 332.

21. Державний стандарт України (ДСТУ) 3396.2-97. “Технічний захист інформації. Терміни та визначення”. URL: http://www.online.budstandart.com/ua/catalog/doc-page.html?id_doc=69175

22. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДІП НАПрН України). Київ: ТОВ “Видавничий дім “АртЕк”, 2019. 288 с.

~~~~~ \* \* \* ~~~~~

## Правова інформатика

УДК 34:001.895:004(045)

**ВАРАВА І.**, старший викладач кафедри теорії та історії держави і права,  
Національний авіаційний університет.

### ІННОВАЦІЇ У ПРОФЕСІЙНІЙ ДІЯЛЬНОСТІ ЮРИСТІВ: ВИКОРИСТАННЯ ПОТУЖНОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ

**Анотація.** Сучасний етап розвитку суспільства – це насамперед широкий ринок цифрових технологій, що постійно охоплює нові галузі виробництва. Цей ринок активно розвивається, передові інформаційно-комунікаційні технології проникають в інші сфери виробництва та суспільної діяльності, що зумовлено прогресом технологічного сектору. Не є винятком і така сфера людської діяльності, як юриспруденція. У статті висвітлена проблематика професії юриста, що властива для сучасної України. Акцентовано увагу читача на актуальності впровадження інновацій в діяльність українських правників, зумовлених процесами глобалізації.

**Ключові слова:** юрист, штучний інтелект, інноваційні технології, юридичний аутсорсинг, фрілансер, прогностична функція штучного інтелекту.

**Summary.** The modern stage of development of society, first of all, is the wide market of digital technologies that covers all new industries of production constantly. This market develops actively, it frontlines of ICT get to other spheres of production and public activity, that predefined by technological sector progress. Such sphere of human activity as jurisprudence it is not an exception. The article covers the lawyer profession problems peculiar to modern Ukraine. The attention of the reader is emphasized on the urgency of introducing innovations into the activity of Ukrainian lawyers, caused by the processes of globalization.

**Keywords:** lawyer, artificial intelligence, innovative technologies, legal outsourcing, freelancer, predictive function of artificial intelligence.

**Аннотация.** Современный этап развития общества – это прежде всего широкий рынок цифровых технологий, который постоянно охватывает все новые отрасли производства. Этот рынок активно развивается, передовые информационно-коммуникационные технологии активно проникают в другие сферы производства и общественной деятельности, что обусловлено прогрессом технологического сектора. Не является исключением и такая сфера человеческой деятельности, как юриспруденция. В статье освещена проблематика профессии юриста, характерная для современной Украины. Акцентировано внимание читателя на актуальности внедрения инноваций в деятельность украинских юристов, обусловленных процессами глобализации.

**Ключевые слова:** юрист, искусственный интеллект, инновационные технологии, юридический аутсорсинг, фрилансер, прогностическая функция искусственного интеллекта.

**Постановка проблеми:** У статті піднято сучасні проблемні питання професійної діяльності юриста, актуальність яких зумовлена появою та використанням в юридичній практиці штучного інтелекту. Такими проблемами сьогодні є: безпека для всіх учасників правових відносин, візуалізація штучного інтелекту в глобальну юридичну базу даних, якісне оновлення наукової та суспільної свідомості, швидкий пошук інформації та підвищення продуктивності юридичної діяльності, покращення процесу прийняття рішень, мобільність надання юридичних консультацій, здешевлення юридичних послуг, ефективність проведення спеціальних експертиз, тощо.

Адвокати та їх клієнти зможуть безпечно обговорювати питання в Інтернеті, завантажувати та передавати документи для перегляду, створювати юридичні документи та здійснювати інші бізнес-операції, пов'язані з доставкою юридичних послуг у безпечному цифровому середовищі. Таке явище зазвичай називають “віртуальною юридичною фірмою”, “веб-практикою закону” чи “он-лайн-практикою”.

**Мета статті** – охарактеризувати інноваційні процеси в правничій діяльності, дослідити шляхи модернізаційної трансформації юриста-фахівця до новітніх життєвих реалій, що характеризуються динамічним розвитком інформаційно-комунікаційних технологій (далі – ІКТ) і штучного інтелекту (далі – ШІ) та постановка конкретних завдань і вимог до співпраці сучасних юристів з ШІ.

*Завданням статті* є визначення сучасних проблемних питань професійної діяльності юриста та акцентування уваги науковців на потребі підготовки і розробки ґрунтовного правового поля, яке б опиралось на засади гуманізму та розумної співпраці зі штучним інтелектом і гарантувало реальний захист прав людини та враховувало всесвітні глобалізаційні процеси цієї сфери.

*Актуальність і новизна роботи.* У статті визначено переваги активного впровадження у практичну діяльність юриста-фахівця потужностей штучного інтелекту та інноваційних комп'ютерних технологій. Аргументовано пропонується співпраця юриста зі штучним інтелектом для досягнення поставленої даною професією мети – досягнення правопорядку та утвердження в суспільстві людиномірних цінностей та здійснено мотивацію дослідників у сфері права до нових наукових розвідок на основі науково-прогностичного методу дослідження.

**Результати аналізу наукових публікацій.** Проблема співпраці юриста зі штучним інтелектом правовою наукою досліджена недостатньо. Нами опрацьовані наукові розвідки суміжних напрямків, в яких здійснено теоретико-правовий підхід до даної проблематики. Особливо цікавими з теоретичної точки зору є наукові роботи Гадомського Д. [2], Кравчук С. та Боровікова В. [3], Приймачук Ю. [4], Родюк А. [5], які досліджували проблематику та розвиток ІТ-права в Україні. Є також теоретико-правові розробки з питань інформаційної безпеки, в т. ч. за співпраці зі штучним інтелектом таких дослідників як Хмарський М., Чута. І., Підгайний М., Удовиченко А., Гадомський Д., Полатайко М. [6].

**Виклад основного матеріалу.** Глобалізаційні процеси кінця ХХ – початку ХХІ століть, посилені стрімким розвитком і широким поширенням інформаційно-комунікаційних технологій, зумовили низку масштабних змін у різних сферах сучасного суспільства. Україна, рухаючись за вектором інтеграції до Європейського Союзу, синхронно переходить до суспільства знань, адже Євросоюз ще наприкінці минулого століття обрав свій інформаційно-технологічний шлях модельного розвитку. А виконання основних положень Угоди про Асоціацію між Україною та ЄС передбачає адаптацію правових основ інформаційного суспільства в Україні до європейських стандартів. Тому якщо Україна прагне заявити про себе на політико-правовій карті світу як інформаційно-технологічно орієнтована країна, то їй належить кардинально змінити спосіб життя більшої частини населення через впровадження механізму правового регулювання інформаційного суспільства. Стає важливою необхідність створення ефективної системи забезпечення прав і свобод громадян та соціальних інститутів на вільне отримання, поширення і використання інформації та знання як найважливішої умови демократичного розвитку, щоб запобігти самотійному розвитку та формуванню неконтрольованого інформаційного суспільства в Україні. Право має відповідати на всі виклики та загрози інформаційного суспільства.

Юрист за сучасних умов вимушений виховувати в собі багатофункціональність та відходити від вузької спеціалізації й жити “в ногу з часом”, постійно розумово та професійно самовдосконалюючись. Неминуче виникає потреба використання потенціалу штучного інтелекту у роботі юриста та розробки таких інноваційних продуктів, що покликані впорядкувати суспільні і індивідуальні відносини.

Ключову роль у складі компетентностей ХХІ сторіччя відіграють технологічні та соціальні навички, навички мислення та набуття знань високого рівня, комунікативність та здатність до співпраці. Визначальними показниками рівня підготовки сучасного фахівця є навички взаємодії з засобами ІКТ, пошуку потрібних відомостей, їх критичного оцінювання і використання. Технологічна революція у правовій сфері знаходиться в активній фазі і боти-юристи – нині вже реальність.

Динамічний розвиток високих технологій та автоматизації, розширення можливостей доступу до інформації – усе це вимагає гнучкого реагування на новітні зміни, нових знань і навичок, в тому числі й від юристів. Перед юристом майбутнього постають такі мультизадачі: продукувати нестандартні розв’язання проблем, оперативно реагувати на будь-які загрози, прогнозувати можливі майбутні ситуації. Це вимагає від фахівців-правників уміння виважено ризикувати, мати здатність до взаємодії й комунікації, в т. ч. тісно співпрацювати зі штучним інтелектом [3].

Сучасні роботодавці оцінюють фахівців не лише за рівнем знань і професійних навичок, а й за вмінням постійно інтелектуально самовдосконалюватися. Тому класичні форми викладання не є достатньо ефективними та потребують застосування інноваційних методик і нових наукових розробок. Сьогодні такі новітні технології як: *Google*-сервіси, мобільні засоби, електронні бібліотеки, соціальні спільноти, електронна пошта, освітні інформаційні мережі, технології віртуальної навчальної діяльності, навчальнометодичні комплекси дисциплін відносяться до мережних технологій відкритих систем.

В правовому житті нашої країни до послуг юристів широка кон’юнктура мобільних додатків, онлайн-конструкторів договорів, аналітичних он-лайн-платформ, смарт-офісів юридичних фірм. Донедавна здавалося, що роботи ніколи не замінять людей у таких сферах як юриспруденція, але сьогодні ми є свідками того, як все змінюється. Завдяки роботизації та цифровим технологіям вже автоматично здійснюється аналіз документів (наприклад, складання договорів, позовів, тощо). Додаток на основі алгоритмів *DoNotPay* допомагає визначити випадки, коли водієві не потрібно оплачувати штраф за парковку. Більше того, функції сервісу значно розширилися і, завдяки додатку, користувачі мають можливість отримати консультації про те, як правильно заповнити форму для виходу у декрет або як поводитися, якщо орендодавець порушив договір. Такий сервіс доступний для використання в Англії і США та названий “першим в світі роботом-юристом, який допомагає відповісти на запитання в тисячі областей” [2]. Послуги штучного інтелекту є досить ефективними у проведенні спеціальних експертиз, що є надзвичайно важливим в юридичній практиці [4]. Як відомо, один з найбільш громіздких аспектів в юридичній практиці – дослідження та пошук інформації. Зазвичай юристу необхідно вивчати та аналізувати історії клієнтів, проводити брифінги, досліджувати звіти і свідчення, для пошуку того, що допоможе виграти справу. Використовуючи ресурси штучного інтелекту, сьогодні юристи можуть знайти найбільш важливу інформацію дуже швидко. На *AngelList* розміщені 729 компаній, які спрощують роботу юристам і полегшують життя користувачам [5].

Сучасні правники раді вітати прогрес технологій і у сфері інформаційної безпеки, оскільки конфіденційність має першорядне значення в їх роботі, а проблема безпеки юридичних фірм є дуже актуальною.

Надзвичайна мобільність сучасного суспільства, життя “на ходу”, призводить до того, що фахівці-юристи працюють мобільно зі смартфона. За такої ситуації важко переоцінити роль мобільних додатків, які покращують взаємодію з клієнтом і прискорюють реакцію на запити, заощаджують час і звільняють фахівця від необхідності постійно бути біля комп’ютера в офісі.

Вартий уваги і такий додаток, як *Business Intelligence*, що обробляє великі масиви інформації і візуалізує тенденції. Крім того, автоматично розсилаються у простому графічному вигляді тренди і показники роботи компанії всім співробітникам. Менше часу витрачається на організацію даних, створення звітів і аналіз чисел.

Передові компанії і державні інституції світу активно інвестують у перспективні цифрові технології, такі як мобільні засоби комунікації, мережні соціальні медіа, системи аналізу *Big Data* (“Великих Даних”), “інтелектуальні” пристрої, тощо. Серед них особливу роль відіграють “Хмарні технології (сховища)”, що використовують організації по всьому світу, і це зростання відбувається вражаючими темпами. “Хмара” дозволяє фірмам отримувати необмежений доступ до ІТ-інфраструктури та платити тільки за ті функції, які дійсно необхідні. Розробники Хмарних сховищ і сервісів постійно працюють над підвищенням рівня безпеки (захисту конфіденційності інформації), тому все більше юридичних фірм активно освоюють цифрові тенденції. Якщо у юридичної фірми немає великого штату техпідтримки, щоб підтримувати безпеку програмного забезпечення на локальних комп’ютерах, “хмара” теж стає виходом, адже навіть одна застаріла програма на комп’ютері юриста може стати лазівкою в системі безпеки всієї фірми.

Більш того, у сфері ІКТ спостерігається тенденція щодо конвергенції новітніх технологій. Тобто, сьогодні різноманітні технології, кожна з яких на початку створення передбачала конкретне функціонально-цільове призначення, вже застосовують можливості інших технологій, які інтегруючись стали доповнювати одна одну і у комплексі створювати, так би мовити, надсумарний ефект конвергентності та надавати нову якість результатів від сумісного їх використання [7].

Переваги новітніх ІКТ та штучного інтелекту очевидні: вони повністю змінюють спосіб життєдіяльності і мислення, допомагають заощаджувати час і гроші, автоматизують рутинні процеси і дозволяють фахівцям концентруватися на дійсно важливих завданнях. Завдяки інноваційним технологіям юристи отримують можливість не бути “прив’язаними” до офісів та самостійно визначати свій робочий графік.

Перспективні ІКТ є ефективним інструментом реалізації рівного доступу до навчання. Хмарні технології найбільшою мірою відповідають потребам вирішення нагальних соціально-економічних, освітньо-культурних проблем сучасного суспільства та вирішення багатьох проблем галузі юриспруденції. Основні з яких – підвищення рівня доступності та якості освіти, взаємозв’язку процесів наукових досліджень і підготовки кадрів, формування й забезпечення функціонування освітньо-наукового середовища вищих навчальних закладів.

Реалізація відкритого навчального середовища для майбутніх юристів відбувається через застосування у практичній діяльності мережних технологій відкритих систем. Це допомагає формувати особистість, здатну творчо та глибоко мислити, раціоналізувати перспективні ідеї та їх реалізацію в професійній діяльності, а також сприяє активізації фундаментальної підготовки фахівців, адаптації до швидкісних темпів розвитку

інформаційного суспільства, створює сприятливі умови для опанування обраної професії. Тобто, йдеться про підготовку всебічно розвинених фахівців, які вміють самоутверджуватися і розкриватися, приймати рішення в складних умовах, поєднувати особисті інтереси з суспільними.

Одним із основних новітніх джерел для дистанційного навчання і фахового самовдосконалення є наукові та навчальні блоги. На таких блогах, як, наприклад, *dreamdoschools*, *eliademy* та ін. відбувається обмін інформацією, досвідом, що підвищує пізнавальну самостійність і мотивує користувачів до самовдосконалення. Ефективною буде робота в сучасних середовищах програмування таких як *Scratch*, *Screm*.

Сьогодні розвитку інноваційних юридичних проєктів в Україні сприяє Гаазький інститут інновацій в праві (HiiL). Варто відмітити, що протягом останніх двох років в Україні було виділено €150 тис. для фінансування стартапів у сфері права. У міжнародному контексті Україна виглядає як перспективна екосистема з технологіями, що подають великі надії. Тут за останні пару років на ринку з'явилося чимало legal tech проєктів. Ось кілька прикладів [1].

- Бот *Open DataBot* – відстежує зміни в реєстраційних даних бізнесу та стежить за судовими виписками.
- Додаток *Karatel* – сприяє боротьбі з корупцією. Навіть якщо користувач не знає юридичних тонкощів ситуації, сервіс дасть відповідь зрозумілою мовою.
- Бот *& Partners* – формує договір на розробку програмного забезпечення, NDA і відповідь на найбільш поширені питання IT-фахівців прямо в месенджері.
- Ресурс *AxDraft* – може підготувати цілий пакет договорів для великих бізнес-угод. Від вас необхідно лише надати ключову інформацію в декількох полях.
- Телеграм-бот *OblavaBot* – допомагає представникам бізнесу в пошуку і виклику адвокатів відповідної спеціалізації на слідчі дії.
- Он-лайн-ресурс “суд на долоні” – стане в нагоді при роботі з Єдиним держреєстром судових рішень.
- *Dom Jurista Analytics* – прогнозує результати розгляду справи в суді, ґрунтуючись на індивідуальному аналізі ситуації. Користувачі отримують незалежний висновок у справі.
- *EasyTender* – проєкт, який допомагає бізнесу вигравати в тендерах і відстоювати свої права в державних закупівлях без корупційної складової.

Англійські дослідники вважають, що завдяки новітнім технологіям, серед яких *Big Data*, автоматизоване складення документів, онлайн-правосуддя, штучний інтелект, вартість юридичних послуг зменшиться. “Рано чи пізно спори будуть вирішуватися за допомогою віртуальних судів або так званого “он-лайнового правосуддя” [5].

Ще один фактор, що суттєво вплине на юридичну професію в майбутньому, який відзначили в *The Law Society*, – це взаємовідносини “клієнт-юрист”. Вже сьогодні в Україні мова йде про те, що від юридичного радника клієнт очікує не вирішення точкових проблем, з якими він звертається, а готове, комплексне бізнес-рішення. Це означає, що юрист має бути не лише професіоналом в певній галузі права, а ще й експертом в області, де веде бізнес його клієнт, аналітиком та менеджером [2].

Ще одним елементом забезпечення ефективних взаємовідносин між клієнтом та юрфірмою в дослідженні *The Law Society* було названо системи *CRM (Customer Relationship Management)* – прикладне програмне забезпечення, покликане забезпечити автоматизацію взаємодії з клієнтами. Дана система дає можливість керувати клієнтською базою юридичної фірми, вести облік вхідних запитів, керувати проєктами з

можливістю побачити ефективність кожного співробітника, робити автоматичні e-mail та SMS-розсилки [5].

Однією з проблемних тенденцій в майбутній роботі юриста буде щоденна і постійно зростаюча конкуренція. Можна спрогнозувати, що у майбутньому ми матимемо ситуацію, за якої юридичні та фізичні особи зможуть знаходити правовий шлях до розв'язання проблем власними силами, користуючись послугами юридичного аутсорсингу лише за крайньої необхідності. Щодо професії юриста – то важливими стануть не професійні уміння, якими володіє фахівець, а його здатність використовувати і ефективно комбінувати весь комплекс своїх вмінь для колективного вирішення складних завдань. Це в свою чергу може призвести до появи нових так званих “гібридних професій”. При цьому юристи поповнять ряди фрілансерів, що ми спостерігаємо вже сьогодні, та об'єднують вузьких спеціалістів у проектні групи використовуючи *coworking*-платформи. Проте, звичайно, ніякі сучасні технології не зможуть замінити юриста-професіонала, як посередника у переговорах, аналітика та мудрого медіатора [6].

Як бачимо, існує нагальна потреба розробки нових методів набуття знань та практичних навичок для юристів майбутнього у сфері інноваційних технологій та ІІІ. Саме тісна співпраця юриспруденції з інноваційними технологіями та штучним інтелектом уможливить створення в Україні таких глобальних інноваційних продуктів, які допоможуть зробити життя безконфліктним, впорядкованим і злагодженим.

Штучний інтелект вже сьогодні є частиною об'єктивної дійсності, яка з кожним днем набуває відповідних соціологічних та правових форм.

Надшвидкі темпи розвитку комп'ютерної техніки та інформаційних технологій ХХІ ст. змінили сприйняття людиною поняття інформації. Інформація стала основним ресурсом і стрімко проникла у всі сфери людської життєдіяльності. Продовжується процес формування так званого інформаційного суспільства. Підвищується важливість інформації, її якості та швидкості доступу до неї. Крім того, глобалізаційні тенденції, які характеризують сучасну епоху, найбільш проявляються саме в інформаційній сфері, забезпечуючи діалог культур і цивілізацій у всіх без виключення напрямках життєдіяльності людства.

Важливу роль у цих процесах покликано відіграти право, яке має впливати на хід вказаних процесів.

Швидкий розвиток мережевих та Хмарних технологій, телекомунікацій, потужностей штучного інтелекту значно розширили можливості використання ІКТ у всіх сферах життєдіяльності. Поширення використання ІКТ у повсякденному житті призвело не тільки до початку нової суспільної ери – інформаційного суспільства, але й до необхідності правового врегулювання цього невідворотного та неминучого процесу.

Нині в Україні головним пріоритетом держави визначено прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал, сприяючи суспільному і особистому розвитку та підвищуючи якість життя.

Україна, маючи свою гідну історію такої сфери, як кібернетика, готує і має значну кількість висококваліфікованих фахівців з інформаційно-комунікаційних технологій, математики, кібернетики; у країні постійно зростає та поновлюється парк комп'ютерної техніки, сучасних систем та засобів телекомунікації, зв'язку; високою є ступінь інформатизації банківської сфери.

Проте потрібно відмітити недостатній ступінь розбудови інформаційного суспільства в Україні порівняно із світовими тенденціями.

Існують конкретні причини такого незрозумілого відставання: відсутня координація зусиль державного і приватного секторів економіки з метою ефективного використання наявних ресурсів; неефективним є використання фінансових ресурсів, спрямованих на інформатизацію; недостатній розвиток нормативно-правової бази інформаційної сфери; повільно відбувається створення інфраструктури для надання інформаційних послуг з використанням мережі Інтернет; недостатній рівень комп'ютерної та інформаційної грамотності населення, повільне впровадження нових методів навчання із застосуванням сучасних інформаційно-комунікаційних технологій; низький рівень інформаційної представленості України в Інтернет-просторі, і недостатня присутність україномовних інформаційних ресурсів; також недостатній рівень державної підтримки виробництва засобів інформатизації, програмних засобів та впровадження ІКТ, що не забезпечує всіх потреб економіки і суспільного життя; та інші.

На жаль, існують проблеми у питанні захисту авторських прав на комп'ютерні програми, тож для прискореного розвитку інформаційного суспільства в Україні необхідні державні рішення, спрямовані на створення національних інноваційних структур (центрів, технополісів і технопарків) з розробки конкурентоспроможного програмного забезпечення.

Основними стратегічними цілями розвитку інформаційного суспільства згідно чинного законодавства в Україні є:

- прискорення розробки та впровадження новітніх конкурентоспроможних ІКТ в усі сфери суспільного життя;
- забезпечення комп'ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх інформаційно-комунікаційних технологій у формуванні всебічно розвиненої особистості;
- розвиток національної інформаційної інфраструктури та її інтеграція із світовою інфраструктурою;
- державна підтримка нових “електронних” секторів економіки (торгівлі, надання фінансових і банківських послуг тощо);
- створення загальнодержавних інформаційних систем;
- збереження культурної спадщини України шляхом її електронного документування;
- державна підтримка використання новітніх ІКТ засобами масової інформації;
- використання ІКТ для вдосконалення державного управління, відносин між державою і громадянами;
- захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту персональних даних, та мінімізації ризику “інформаційної нерівності”;
- вдосконалення законодавства з регулювання інформаційних відносин;
- покращення стану інформаційної безпеки в умовах використання новітніх ІКТ.

Підсумовуючи, варто сказати, що сьогодні законодавча та нормативно-правова база функціонування інформаційної сфери України потребує узагальнення та систематизації національного інформаційного законодавства шляхом кодифікації – розробки системоутворюючого кодексу – Інформаційного кодексу України.

### **Висновки та пропозиції.**

Наведене в статті окреслення “білих плям” професійної діяльності юриста спонукає до пошуку нових шляхів вирішення певних кризових моментів його професійної діяльності.

Мобільні додатки для юристів, он-лайн-конструктори договорів, аналітичні он-лайн-платформи, смарт-офіси юридичних фірм – все це вже активно функціонує в правовому житті нашої країни. Хоча технології у сфері права стикаються з серйозними проблемами на кшталт негативного ставлення традиційних гравців (через дешевизну надаваних додатками консультацій) або труднощів захисту даних та інформації, вже ясно, що технологічний прогрес увійшов в галузь юриспруденції назавжди. Співпраця юриста зі штучним інтелектом сприяє досягненню поставленої даною професією мети – забезпечення правопорядку та утвердження в суспільстві людиномірних цінностей.

Метою інновації має бути не заробляння грошей, а забезпечення доступу до правосуддя. Серед позитивів від впровадження інновацій – підвищення якості надання юридичних послуг та підвищення рівня доступності правосуддя.

Нині в Україні головним пріоритетом держави визначено прагнення побудувати розвинене інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними, щоб надати можливість кожній людині повною мірою реалізувати свій потенціал.

Саме тісна співпраця юриспруденції з ІКТ та штучним інтелектом уможливить створення в Україні таких глобальних інноваційних продуктів, які допоможуть зробити життя безконфліктним, впорядкованим і злагодженим.

Підсумовуючи викладене вище, можна сказати, що в Україні упродовж останніх років напрацьовано низку законодавчих актів, які регулюють відносини, що виникають в інформаційному суспільстві. Однак доводиться констатувати, що в сучасних умовах розвитку суспільства інформаційне законодавство потребує якісних змін. За всією його розгалуженістю воно залишається суперечливим, належним чином не систематизованим і не кодифікованим.

### Використана література

1. URL: <https://www.radako.com.ua/news/innovaciyi-v-pravi-koli-algoritmi-zaminyat-yuristiv>
2. Гадомський Д. (2019) І до ворожки не ходи: майбутнє юридичної професії. URL: <https://www.axon.partners/uk/blog/i-do-vorozhki-ne-hodi-maybutne-yuridichno>
3. Кравчук С., Боровікова В. (2019) Юрист майбутнього – в співпраці з штучним інтелектом. URL: <https://www.ukrlogos.in.ua>
4. Приймачук Ю. (2019). Кіберпанк для юристів: що потрібно знати про штучний інтелект. URL: <https://www.gurt.org.ua/news/informator/55834>
5. Родюк А. (2019). Огляд ЗМІ: про майбутнє юридичної професії. URL: <https://www.radako.com.ua/news/oglyad-zmi-pro-maybutnie-yuridichnoyi-profesiyi>
6. Хмарський М., Чута. І., Підгайний М., Удовиченко А., Гадомський Д., Полатайко М. (2018). Нові професії в юриспруденції. URL: <http://www.yur-gazeta.com/publications/practice/inshe/novi-profesiyi-v-yurisprudenciyi.html>
7. Брижко В.М., Фурашев В.М. Конвергенція новітніх технологій: стан і перспективи змін у інформаційних відносинах. *Інформація і право*. № 1(20)/2017. С. 51-67.

~~~~~ \* \* \* ~~~~~

Інформаційна і національна безпека

УДК 342.7

КОРЖ І.Ф., доктор юридичних наук, с.н.с., завідувач наукової лабораторії
НДІ інформатики і права НАПрН України.
ORCID: <https://orcid.org/0000-0003-0446-5975>.

КОНЦЕПТУАЛЬНІ ЗАСАДИ ПРАВОВОЇ БЕЗПЕКИ

Анотація. В даній статті досліджується питання концептуальних засад поняття “правова безпека”, особливості цього поняття, що характеризують зазначений феномен, і що у підсумку дозволяє визначити сутність і його зміст, виходячи з загальнотеоретичних позицій. Показана відмінність змісту зазначеного поняття від змісту поняття “юридична безпека”. Визначено місце “правової безпеки” в системі інших видів безпеки, розкрито співвідношення їхніх сутності та змісту; досліджено та визначено його суб’єкти та об’єкти, механізми і напрями забезпечення зазначеної безпеки. Наводяться недоліки у реалізації та забезпеченні прав громадян, пропонуються шляхи їх вирішення.

Ключові слова: оперативно-виконавча діяльність, право, правова безпека, правотворча, правозастосовна та правоохоронна діяльність.

Summary. This article analyzes conceptual foundations of the concept of “legal security”, the features of this concept that characterize this phenomenon, which allows to determine the essence and content of the concept of “legal security”, based on general theoretical positions. The difference between the content of this concept and the content of the concept of “juridical security” is shown. The place of “legal security” in the system of other types of security is determined, the correlation of their essence and content is disclosed; its subjects and objects, mechanisms and directions for ensuring the specified security were investigated and determined. Examples of shortcomings in the implementation and enforcement of citizens’ rights are given, and ways to address them are proposed.

Keywords: operational and executive activity; right; legal security; law-making activity; enforcement activities; law protection activities.

Аннотация. В данной статье исследуется вопрос концептуальных основ понятия “правовая безопасность”, особенности этого понятия, характеризующие указанный феномен, что и позволило определить сущность и его содержание, исходя из общетеоретических позиций. Показано отличие содержания этого понятия от содержания понятия “юридическая безопасность”. Определено место “правовой безопасности” в системе других видов безопасности, раскрыто соотношение их сущности и содержания; исследованы и определены его субъекты и объекты, механизмы и направления обеспечения указанной безопасности. Приводятся примеры недостатков в реализации и обеспечении прав граждан, предлагаются пути их решения.

Ключевые слова: оперативно-исполнительная деятельность, право, правовая безопасность, правотворческая, правоприменительная и правоохранительная деятельность.

Постановка проблеми. Відповідно до положень статей 3, 8, 21 і 22 Конституції України [1]: “людина, її життя і здоров’я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави. В Україні визнається і діє принцип верховенства права. Права і свободи людини є невідчужуваними та непорушними. Конституційні права і свободи людини і громадянина, закріплені в Конституції, не є вичерпними”.

Питанням прав і свобод громадян в науковій літературі приділено значну увагу, різні його аспекти досліджено в роботах В.Б. Авер'янова, В.В. Речицького, П.М. Рабіновича, С.Г. Серьогіної, Ю.М. Тодики, М.В. Цвіка, О.О. Чуб та інших. Водночас концептуальний характер дослідження цього права, насамперед через призму правової безпеки, особливостей її здійснення вимагають продовження наукових досліджень.

У 2005 році науковим дослідником Добродумовим П.О. було вперше зроблено спробу надати визначення терміну “правова безпека”. Ним була звернена увага на фактори, які негативно впливають на правову систему, знижують ефективність її дії і обумовлюють необхідність забезпечення її безпеки. Серед них – недосконалість чинного законодавства, його нестабільність, процесуально-правовий нігілізм, порушення і навіть невиконання законів, низький рівень правової культури. Пізніше у 2009, 2013, 2018 роках цьому питанню у відповідних аспектах приділили увагу дослідники Корж І.Ф., Лобода А.М.

Тому нинішня спроба розглянути правову безпеку не сегментно, а концептуально, є певним науковим кроком вперед у вивченні даного феномена.

Метою статті є вирішення питання концептуальних засад поняття “правова безпека”, його особливості, що характеризують зазначений феномен, і що у підсумку дозволяє визначити сутність і його зміст, виходячи з загальнотеоретичних позицій; показати відмінність змісту зазначеного поняття від змісту поняття “юридична безпека”; уявити місце “правової безпеки” в системі інших видів безпек; розкрити співвідношення їхніх сутності та змістів; визначити його суб'єкти та об'єкти, механізми і напрями забезпечення зазначеної безпеки.

Виклад основного матеріалу. В ст. 1 Конституції України зазначено, що “Україна є суверенна і незалежна, демократична, соціальна, правова держава” [1]. Правова держава – це суверенна, політико-територіальна організація публічної влади, яка ґрунтується на принципах поваги і законодавчого визнання прав і свобод людини, законності, верховенства права.

Ознаками України як правової держави є:

- 1) верховенство права (ст. 8 Конституції України);
- 2) беззаперечне визнання і нормативне утвердження суверенітету народу як єдиного джерела публічної влади;
- 3) нормативне врегулювання і практичне забезпечення реалізації принципу поділу державної влади на законодавчу, виконавчу і судову;
- 4) забезпечення і гарантія основоположних прав, свобод і законних інтересів людини та громадянина;
- 5) взаємодія особи і держави на основі дотримання принципу: “Фізичній особі дозволено робити те, що прямо не заборонено законом. Юридичній особі дозволено робити тільки те, що прямо дозволено законом”. Наприклад, органи державної влади та органи місцевого самоврядування, їх посадові особи зобов'язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України (ч. 2 ст. 19 Конституції України) [1];
- 6) рівність усіх індивідів, громадян перед законом і судом;
- 7) політична багатоманітність;
- 8) максимальні гарантії прав і свобод людини і громадянина;
- 9) здійснення державою і громадянами (громадянським суспільством) взаємного ефективного контролю й нагляду за реалізацією законів і дотриманням принципу верховенства права;

10) визнання міжнародних правових актів, зокрема в частині закріплення прав і свобод людини та громадянина, частиною національного законодавства (ст. 9 Конституції України) [1];

11) взаємна відповідальність особи і держави за свою діяльність;

12) високий рівень правосвідомості та правової культури громадян.

Таким чином, в Україні є достатні нормативні умови, необхідні для формування повноцінної правової держави. Незважаючи на те, що Конституція України проголосила Українську державу правовою, проте цю конституційну норму необхідно сприймати як норму-мету, оскільки державу такого ґатунку ще потрібно побудувати.

Конституція України визнає народ носієм суверенітету і єдиним джерелом влади в Україні. Український народ здійснює владу безпосередньо, через органи державної влади і органи місцевого самоврядування (ч. 2 ст. 5 Конституції України) [1].

Народовладдя є вираженням демократії. З правової точки зору, народовладдя означає приналежність усієї суспільної влади, в тому числі державної, народові, вільне здійснення народом цієї влади відповідно до його суверенної волі в інтересах як всього суспільства, так і кожної людини й громадянина. Визнання народу верховним носієм державної влади є вираженням народного суверенітету. Це означає, що народ, не поділяючи ні з ким своєї влади, здійснює її самостійно і незалежно, виключно в своїх інтересах. Право народу на встановлення і здійснення влади є його природним правом, а відтак народний суверенітет – невідчужуваний і недоторканий. Іншими словами, ніхто не може узурпувати державну владу.

Народовладдя реалізується через безпосередню (пряму) демократію і представницьку (непряму) демократію.



Із зазначеного випливає, що регулятором демократії є право, джерелом якого, у свою чергу, є первинні і вторинні його джерела. Первинні з них містять правові норми, що мають обов'язкову юридичну силу. До таких джерел зазвичай відносять нормативно-правові акти, міжнародно-правові договори та правові звичаї, причому звичаї зазвичай поступаються пріоритетністю.

До вторинних джерел у країнах романо-германського права відносять раніше ухвалені судові рішення, яким надається прецедентний характер, та правову доктрину. Ці джерела відіграють допоміжну роль та не є достатньою юридичною базою для ухвалення судових рішень.

Таким чином, саме право, через застосування його складової – правової норми, є тим механізмом, який має забезпечувати ефективне функціонування у державі демократії та народовладдя – зокрема, та функціонування і подальший розвиток соціальної системи – в цілому.

Норми права є тими механізмами-регуляторами суспільних відносин, що виникають і функціонують у процесі реалізації основоположних (конституційних) прав і свобод особи, так само як і фактично в усіх сферах життєдіяльності [2]. Зазначені суспільні відносини, які виникають і діють в процесі здійснення влади народом, тобто здійснення народовладдя, є основним предметом правового регулювання конституційного права. Такі відносини опосередковуються правовими нормами, які складають зміст найважливіших джерел конституційного права – Конституції України, Декларації про державний суверенітет України [3], конституційних законів тощо.

Окрім регулювання суспільних відносин, право є універсальним механізмом забезпечення як національної безпеки – в цілому, так й усіх видових безпек – зокрема. Правові засоби забезпечення національної та інших видів безпек переслідують двояку мету:

- ефективне функціонування чинного права та реалізація його нормативних можливостей в межах міжнародного і національного правового порядку;
- напрацювання нових правових норм з метою ефективного захисту інтересів особи, суспільства і держави та їхніх інституцій [4].

Від стану дієвості та ефективності регулювання суспільних відносин права залежить дієвість і безпека функціонування та подальший розвиток будь-якої соціальної системи. А зазначені критерії можуть бути належними за умови перебування самої системи права в стані, за якого право успішно здійснює свою місію, тобто перебуває у належному, безпечному стані. Таким чином з'являється така самостійна правова категорія – як “правова безпека” [5], якій приділяється дедалі більше уваги з боку українських та зарубіжних науковців [6].

Серед суб'єктивних прав людини завжди є право на безпеку. Тому право на безпеку можна розуміти як одне із основоположних прав людини. Тобто правова безпека – це самостійний вид соціальної безпеки.

Праву притаманний дуалізм дії, який проявляється в тому, що воно, з одного боку, поряд з політичними, економічними, інформаційними, воєнними та іншими механізмами, є механізмом правового (юридичного) забезпечення національної та інших видів безпеки. З другого боку, право є засадничим визначником подальшого розвитку об'єкту правової безпеки. Саме визначення правом напрямів подальшого розвитку соціальних систем, є тією квінтесенцією сприйняття його певної окремішності і самостійності. З одного боку правова безпека входить до системи різних видів безпек, а з іншого – правова безпека є своєрідним орієнтиром, дороговказом, механізмом забезпечення усіх видів безпек.

Основу поняття правової безпеки складає розуміння умов, джерел, шляхів та механізмів негативного впливу на правову систему (спотворення правових норм, конфлікт норм, утворення правових прогалин, неналежна процедура виконання, ігнорування дії норм, підміна понять, правовий нігілізм, корупція тощо). Сутність правової безпеки зводиться до правового захисту (правового забезпечення) життєво важливих інтересів об'єктів правової безпеки, від негативних впливів, їх недопущення, парирування, або іншими словами мінімізації правових факторів ризиків, викликів, небезпек і загроз.

Предметом захисту системи правової безпеки є життєво важливі інтереси її об'єктів – особи, суспільства і держави в різних сферах життєдіяльності. Для особи – її життєво важливими інтересами є основоположні права і свободи, її життя і гідність, безпечні умови життєдіяльності тощо, які напрацьовані міжнародним правом (Загальна декларація прав людини, Міжнародний пакт про громадянські та політичні права,

Міжнародний пакт про економічні, соціальні і культурні права) і які знайшли своє відображення в Конституції України.

Для суспільства – його життєво важливими інтересами є демократичні цінності, тобто можливість за допомогою права визначати свої політичні, економічні, соціальні та культурні системи; правове забезпечення та брати активну участь у вирішенні питань, що стосуються життя у всій різноманітності його вимірів, добробуту та умов для свого сталого розвитку.

Для держави – її життєво важливими інтересами є: правове врегулювання та захищеність конституційного ладу, суверенітету, територіальної цілісності та недоторканності від існуючих та ймовірних загроз; її території, навколишнього природного середовища – від надзвичайних ситуацій, а також правова система держави, створена на підставі формалізації правових норм (законодавство), які забезпечують належне функціонування держави і визначають напрям її подальшого розвитку.

Державну політику щодо правової безпеки формує парламент, який формалізує норми права в положеннях Основного закону держави – Конституції України, на підставі яких ним же приймаються нормативно-правові акти (закони), якими згадані норми права реалізуються. У свою чергу, систему забезпечення правової безпеки її об'єктів складають відповідні суб'єкти. Суб'єктами забезпечення правової безпеки згаданих об'єктів в Україні є органи виконавчої та судової гілок державної влади. Суди, якими є Конституційний Суд та суди загальної юрисдикції, поновлюють порушені права об'єктів правової безпеки.

Органи виконавчої влади, здійснюючи нормозастосовчу та нормотворчу функції, здійснюють охоронну діяльність згаданих прав, не допускаючи порушення норм права, тобто, безпосередньо забезпечуючи правову безпеку.

Суб'єктами забезпечення правової безпеки в регіонах, тобто на місцях, є органи місцевого самоврядування, які, приймаючи регіональні правові акти реалізують повноваження щодо забезпечення життєво-важливих інтересів об'єктів правової безпеки.

Для ефективного і дієвого забезпечення правової безпеки важливого значення набуває знання факторів негативного впливу та їх відстеження, що дозволяє своєчасно вжити необхідних заходів для їх мінімізації. Як показує практика, існує значна кількість факторів, які суттєво впливають на саме право, на його якісні та сутнісні характеристики. Тому існує об'єктивна необхідність у захисті самого права, усунення стану незахищеності системи права. За характером направленості та ролі суб'єктивного фактора у їх виникненні, можна розрізнити:

– *виклики* – такі характеристики функціонування правової системи, не обов'язково конкретно загрозливого характеру, але які для належного врегулювання суспільних відносин вимагають відповідного реагування на них (становлять приблизно 25 % загроз);

– *ризик* – можливість виникнення несприятливих і небажаних наслідків для функціонування як самої правової системи внаслідок виникнення негативної її характеристики, так і для суспільних відносин, які регулюються правом (становлять приблизно 50 % загроз);

– *небезпеки* – цілком усвідомлена, але не фатальна вірогідність заподіяння шкоди правовій системі, яка визначається наявністю об'єктивних і суб'єктивних факторів дії негативної характеристики на правову систему та на суспільні відносини (становлять приблизно 75 % загроз);

– *загрози* – найбільш конкретна і безпосередня форма дії (впливу) негативного характеру на правову систему та на суспільні відносини (складає 100% настання негативу).

Факторами негативного впливу на об'єкти правової безпеки можуть бути:

- суперечливість і неефективність правових норм, їх економічна незабезпеченість, невідповідність (викривлення, аберація норм) міжнародному праву;
- відсутність необхідних законодавчих актів;
- невідповідність закону праву;
- нестабільність законодавства;
- порушення монолітності правової системи держави;
- прояви правового нігілізму в суспільстві;
- правова безвідповідальність;
- зниження ролі судових органів у правовому врегулюванні;
- прояв високого рівня корупції в суспільстві;
- низький рівень правосвідомості, правової культури, професіоналізму і компетенції законотворчих і правозастосовних органів та їх посадових осіб, що підриває авторитет влади і закону, сприяє свавіллю, розвитку тіньового права, авторитету криміналу, криміналізації відносин;
- недооцінка моральних і правових основ права;
- свавілля судових, правоохоронних та інших державних органів та їх працівників, які покликані вирішувати юридичні конфлікти;
- тривале і неефективне реформування правової системи та державних органів та інше.

Правову безпеку потрібно відрізняти від юридичної безпеки, як особливого різновиду соціальної безпеки. Під юридичною безпекою потрібно розуміти стан правового захисту (забезпеченості, гарантованості) життєво важливих інтересів суб'єктів права у зв'язку з їхнім вступом у сферу правових (юридичних) відносин, тобто мінімізація негативного впливу на функціонування суб'єкта правових факторів ризиків, викликів, небезпек і загроз; здатність юридичними засобами протидіяти зовнішнім і внутрішнім загрозам об'єктивного або суб'єктивного характеру.

Головний вихідний момент юридичної безпеки полягає в захисті від протиправних (незаконних) посягань, або мінімізація їхнього негативного впливу, а також у наявності можливості для подальшого відновлення порушених інтересів в рамках “правового поля”. Правовий (юридичний) захист суспільних відносин у даному випадку є функцією та обов'язком держави, яка для цього створює відповідні органи влади, регламентуючи їхню діяльність в нормативно-правових актах.

Практичний сенс юридичної безпеки полягає в тому, щоб встановити, чи можуть правові норми нормативно-правових актів впливати на виникнення, розвиток і вирішення юридичного конфлікту; яким чином використовувати правовий (юридичний) інструмент для мінімізації та припинення юридичного конфлікту або його попередження з метою забезпечення юридичної безпеки відповідних суб'єктів.

У більшості випадків юридична безпека зводиться, насамперед, до того, щоб нейтралізувати загрози впливу будь-якого небезпечного джерела. Так, юридична безпека держави полягає, насамперед, у тому, щоб забезпечити правову (юридичну) охорону Конституції та існуючих основ конституційного устрою, усунути загрози, які спроможні їх порушити. У свою чергу, юридична безпека особи має певну особливість і полягає не лише в тому, щоб правовими (юридичними) засобами зберегти певну життєво важливу функцію від загроз. Компетентним органам держави необхідно

здійснювати комплекс правових (юридичних) заходів щодо поновлення системи життєзабезпечення, здоров'я, життєдіяльності особи.

Необхідно зазначити, що механізм захисту життєво важливих інтересів об'єктів правової безпеки має формуватися шляхом кропіткої наукової, законотворчої, просвітницької, правозастосовної, організаційної тощо роботи. Імплементация міжнародних правових норм має бути гармонічно вплетена в національну правову матерію шляхом послідовного утворення необхідних соціально-економічних, психологічних, правових та інших базових передумов щодо удосконалення правових механізмів, з одночасним врахуванням особливостей національної правової системи, рівня розвитку соціальних інститутів, правосвідомості тощо.

З огляду на зазначене, захист життєво важливих інтересів об'єктів правової безпеки покладено на державу через правові та інші форми здійснення функцій держави. Це діяльність основних ланок механізму держави, специфічні види державної діяльності, діяльність органів держави, через які реалізуються функції держави і, одночасно, зазначене є напрямками забезпечення правової безпеки.

Під правовими формами здійснення функцій держави розуміється однорідна за зовнішніми ознаками (характеру та юридичними наслідками) діяльність державних органів, пов'язана з виданням юридичних актів. Це – правотворча і правозастосовна діяльність. Правові форми завжди є організаційними щодо здійснення функцій держави.

Правотворча діяльність – це форма здійснення функцій держави шляхом видання нормативно-правових актів, видання, санкціонування, зміни чи скасування правових норм. Ядром зазначеної діяльності законодавча діяльність.

Правозастосовна діяльність – діяльність органів держави щодо виконання Конституції, законів та підзаконних нормативно-правових актів шляхом видання актів застосування права. У зазначеній діяльності виділяються оперативно-виконавча і правоохоронна діяльність.

Оперативно-виконавча діяльність являє собою пов'язану з повсякденним вирішенням різнобічних питань управління справами суспільства безпосередню виконавчо-розпорядчу діяльність державних органів щодо здійснення функцій держави шляхом видання актів застосування норм права, які слугують підставою для виникнення, зміни чи припинення суспільних правовідносин.

Правоохоронна діяльність являє собою форму здійснення функцій держави шляхом здійснення оперативної роботи державних органів щодо охорони норм права від порушень, захисту наданих особам основоположних (конституційних) прав і забезпечення виконання покладених на них юридичних обов'язків.

Внаслідок зазначеної діяльності видаються акти застосування норм права (постанови слідчих, вироки і рішення судів тощо). Специфікою цих актів є те, що вони призначені для профілактики злочинів та інших правопорушень, поновлення порушеного права, реалізації юридичної відповідальності особи, яка здійснила правопорушення, а отже в усіх випадках – в охороні прав особи, захисту інтересів громадян і суспільства в цілому.

Така державна діяльність як судова, охоплює реалізацію функцій держави шляхом здійснення правосуддя усіма складовими судової системи держави – Конституційним Судом, судами (загальними і спеціалізованими). Основні напрями діяльності судів – охорона прав і законних інтересів осіб; охорона правопорядку від злочинних та інших правопорушень; контроль за тим, щоб діяльність державних органів не виходила за правові межі. Так судова влада має право на здійснення контролю за відповідністю

законів Конституції; для захисту прав громадян у їх стосунках з органами виконавчої влади та їх службовими особами тощо.

Виконання вимог суду і виконання його рішень забезпечується силою держави. У разі потреби відповідні органи і посадові особи можуть застосувати відповідні заходи для реалізації рішень і вимог суду. У державному механізмі функціонують спеціальні органи і посадові особи, до обов'язків яких входить забезпечення виконання судових рішень.

Як зазначалося, впорядкування суспільних відносин є необхідною умовою безпеки особи, суспільства і держави, умовою їх функціонування і розвитку. А соціальне призначення права якраз і полягає у врегулюванні, упорядкуванні суспільних відносин, наданні їм належної стабільності, необхідного рівня безпеки. В даному випадку це є характеристикою правового регулювання, його механізму.

В рамках теорії функцій правова безпека розглядалася вище через функції держави. Саме право спрямоване на охорону загальнозначущих, найбільш важливих суспільних відносин, забезпечує їх недоторканність і безпеку, а також безпеку особи, суспільства і держави.

З урахуванням значущості і поширення у праві категорії безпеки, що визначає напрям діяльності права, безпеку можна розглядати і як правовий принцип. Оскільки у праві розглядаються в основному такі основні його принципи, як гуманізм, справедливість, законність тощо, а безпека не згадується, то на нашу думку аналіз безпеки дозволяє стверджувати про її основоположні начала функціонування права.

Поряд з обов'язком держави забезпечити захист життєво важливих інтересів об'єктів правової безпеки, особа має право сама захищати свої основоположні права і свободи від порушень і протиправних посягань будь-якими не забороненими законом засобами (ст. 55 Конституції України) [1] – оскаржувати дії службових осіб, звертатися до ЗМІ, використовувати правозахисні та громадські організації, профспілки, самооборону тощо.

Захист основоположних прав і свобод особи є складним процесом, який, з одного боку, направлений на захист життєво важливих інтересів конкретного об'єкта, реалізацію його свободи щодо розпорядження своїм правом, а з другого – це процес, який має гарантувати дотримання життєво важливих інтересів суспільства і держави. Тому там, де відсутня ефективна система права, держава прагне підпорядкувати своєму впливу і регламентації найбільше складових життя своїх громадян, а тому особа стає незахищеною від свавілля чиновників і протиправності інших осіб і, таким чином, відбувається деградація суспільної правосвідомості.

В різних правових теоріях сам факт різноманіття розуміння права свідчить про те, що з точки зору змісту в “чистому виді”, як таких, безумовно об'єктивних і загальноновизнаних прав і свобод людини не існує. Реальністю є лише уявлення, судження, погляди, теорія про те, що таке права людини, а також політичні, юридичні, моральні та інші норми, що на них базуються. Погляди і норми впливають на матеріальні та духовні можливості і обов'язки людей, які складаються і розвиваються у суспільстві, і опосередковують їх. В цьому сенсі права людини (права особи) спочатку виникають, існують, розвиваються в якості важливого елемента правосвідомості і свідомості в цілому різних соціальних суб'єктів.

З огляду на зазначене, фактично існуючі і як такі, що виникають, соціальні можливості людей визнаються, тлумачаться в якості тих чи інших прав і свобод людини лише в значенні “належного” і, головним чином, – на протигагу об'єктивно можливим і об'єктивно існуючим іншим уявленням, інтерпретаціям, перевагам. Тому саме за таких

умов можливим було як поява самої ідеї прав і свобод людини, поняття “права людини”, так і збереження і підвищення актуальності їх в подальшому тлумаченні.

Поряд з тим різноманітність підходів до прав і свобод людини не применшує можливості і необхідності напрацювання і визнання певного мінімуму загальнолюдських, загальнодемократичних вимог до правового і соціального стану особи. Реалізація цього мінімуму має бути забезпечена незалежно від соціально-політичних, економічних, культурних та інших особливостей конкретної держави. Цей мінімум в якості основоположних прав і свобод людини має бути визнаним усім світовим суспільством незаперечними цінностями. Тому дуже важливо визнати, що на сьогоднішній день цей мінімум універсальних цінностей визнали ще не усі держави і тим паче не усі забезпечують їх фактичну наявність і реалізацію.

Найбільш поширеною є класифікація прав і свобод у відповідності до виділених найбільш важливих сфер суспільного життя, в яких виникають і реалізуються основоположні (конституційні) права і свободи особи, і гарантія дотримання і виконання яких свідчить про стан правової безпеки. Можна виділити чотири великі групи основоположних прав і свобод:

- **політичні** – можливості людини в державному і суспільно-політичному житті, які забезпечують її політичне самовизначення і свободу, участь в управлінні державними справами і прийнятті важливих державних рішень. До них можна віднести право на об'єднання; свобода мітингів, на ходу, демонстрації; право обирати і бути обраним в органи державної влади і місцевого самоврядування; право на доступ до державних посад; право на участь у всенародному обговоренні і голосуваннях (референдумах);

- **особисті** – можливості людини, які не допускають незаконного і небажаного втручання в її особисте життя, яке має забезпечувати існування, своєрідність і автономність особи. Це ті права і свободи, які безпосередньо захищають особисте життя і свободу кожної людини. До них відносяться: право на життя; право на особисту недоторканність; право на повагу, захист честі і гідності; право на недоторканність житла; право на свободу пересування і вибір місця проживання; наявність презумпції невинуватості тощо.

- **соціально-економічні** – можливості особи у сфері виробництва і розподілу матеріальних благ, які покликані забезпечити економічні та пов'язані з ними духовні потреби та інтереси. Це – право на працю; право на відпочинок; право на соціальне забезпечення; право на житло; право спадщини тощо;

- **культурні** – можливості людини користуватися духовними, культурними благами і досягненнями, брати участь у їх створенні у відповідності до своїх здібностей. До них можна віднести: право на користування досягненнями культури; право на освіту; свобода наукової, технічної і художньої творчості тощо. Тут провідним принципом є рівність усіх громадян.

Права й свободи людини і громадянина, закріплені у чинній Конституції України, не є вичерпними. Це означає, що в майбутньому система прав і свобод може бути розширена та вдосконалена. Зазначені права і свободи гарантуються і не можуть бути скасовані. Вони є основоположними тому, що за їх допомогою регулюються найбільш життєво важливі відносини і зв'язки громадянина з державою, які безпосередньо впливають на формування його правового статусу, існують і в різних галузях життєдіяльності, у сфері особистого життя та здійснення індивідуальної свободи.

Правова безпека передбачає захист системи права, законодавства, правової системи в цілому від небезпек і загроз. І в цьому сенсі вона як правове явище забезпечує безпеку

усіх видів безпеки (національну, державну, економічну, екологічну тощо). В силу зазначеного правова безпека займає центральне місце в системі видів безпек, що потребує подальшого наукового дослідження і практичного удосконалення.

Внаслідок глобальних і стрімких змін, що відбуваються у світі, формування системи правових засобів, що утворюють механізм забезпечення правової безпеки, є вкрай актуальним. Неналежна увага до зазначеного призводить до значних соціальних наслідків: правового нігілізму; недовіри громадян до державних, соціальних інститутів; появи синдрому незахищеності особи від порушення своїх прав, що в кінці кінців, стає одною з причин появи і розвитку деструктивних процесів в суспільному розвитку, виникнення соціальних катаклізмів.

Мета механізмів забезпечення правової безпеки – формування за допомогою правових засобів реального забезпечення та гарантування належного правового стану її суб'єктів, що дозволяє подальший їх розвиток.

В наведених тлумаченнях правова безпека практично ототожнюється з такими поняттями, як “ефективна правотворчість”, “правове регулювання”, “правозастосування”, зміст яких наведено вище.

З огляду на зазначене вище терміну “правова безпека” можна надати наступне визначення: *Це стан правової системи, яка завдяки ефективній правотворчості та дієвому застосуванню правових норм в державі спроможна здійснити реалізацію та захист життєво важливих інтересів особи, суспільства і держави, а також створює належні умови для подальшого їх розвитку.*

У свою чергу концептуальним засадам правової безпеки пропонується наступне визначення: *Це система поглядів, певне наукове розуміння такого правового явища, яким є правова безпека, за сутністю, змістом і критеріями, об'єктами і суб'єктами та за напрямками її забезпечення.*

В сучасних умовах в Україні склалася дещо несприятлива для громадян правова реальність, за якої певна частина правових (конституційних) норм не використовується у повному обсязі, частина життєво важливих прав і свобод людини і громадянина перетворилася на гасла, деякі з них не мають механізмів реалізації. Зазначене підтверджується тим фактом, що станом на 1 січня 2020 року Україна знаходиться на третьому місці за скаргами на неї у Європейський Суд з прав людини, поступаючись лише Туреччині та Росії. Серед скарг, що зареєстровані у Європейському Суді з прав людини та чекають на вирішення, майже 15 % містять звинувачення проти української держави. В реєстрі Суду сумарно зареєстровано 59,8 тисяч заяв (на 3,5 тисяч більше ніж торік) [7].

Це дискредитує Конституцію України, підриває довіру до влади, є фактором, що породжує нігілізм громадян. Існують значні невикористані резерви, що мають бути спрямовані на реалізацію пріоритетів соціальної політики і права. Великого значення в цьому зв'язку набуває розвиток необхідної нормативно-правової бази, механізму реалізації прав людини і громадянина, посилення відповідальності суб'єктів права, обмеження впливу олігархічних структур, активна протидія їх зрощуванню з державним апаратом.

Поглиблення соціальної спрямованості правової системи України нерозривно пов'язане з соціокультурними чинниками, із зростанням правової культури та правової свободи особистості та всього суспільства, подолання гіперіндивідуалізму, підвищення соціальної і правової етики, недопущення такого ганебного явища у нормотворчій діяльності в Україні, як аберація. Аберація (інтерполяція – викривлення) правових норм – навмисне чи необережне викривлення, підміна початкових змістів правових норм, а

також формування незапланованих законодавцем правових наслідків, які відбуваються в процесі нормотворчої та правозастосовної діяльності в державі, як на законотворчому рівні, так і в процесі напрацювання підзаконних актів. В Україні є безліч негативних прикладів зазначеного.

Водночас, внаслідок того, що національні правові системи стають більш відкритими одна для одної, створюються умови для вдосконалення законодавства у всіх сферах життєдіяльності суспільства і, передусім, в галузі прав і свобод людини, їх гарантій [8].

Висновки.

Право дедалі більше виступає відповідним мірилом свободи і зміст його полягає в тому, щоб узгодити свободу окремої людини зі свободою інших членів суспільства, дотримуючись принципу рівності. Право виступає як засобом забезпечення свободи, так і істотним засобом обмеження неузгоджених з суспільними потребами і уявленнями людей про добро і справедливість рівня свободи й обсягу влади, створюючи належні засади безпеки усьому живому. Тому поняття “правова безпека”, його сутність і зміст потрібно завжди корелювати зі сутністю і змістом інших видів безпек, зважати на їхню взаємозалежність і взаємовплив один на одного, а також на вихідні, засадничі коріння правової безпеки на сутність та зміст будь-якого виду безпеки.

Використана література

1. Конституція України: Закон України від 26.06.96 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Конституційне право України: підручник; за ред. В.Ф. Погорілка. Київ: Наукова думка, 1999. 735 с.
3. Декларація про державний суверенітет України: Закон України від 16.07.90 р. № 55-ХІІ. *Відомості Верховної Ради УРСР*. 1990. № 31. Ст. 429.
4. Дрейшев Б.В. Правовая безопасность и проблемы ее обеспечения. *Правоведение*. Москва, 1998. № 2. С. 11-19.
5. Тюрина Т.Б. Правовая безопасность в современном Российском государстве (вопросы теории и практики): автореф. дис. ...канд. юрид. наук: 12.00.01. Саратов, 2005. С. 14.
6. Лобода А.М. Правова безпека особи в сучасній українській державі (теоретико-правове дослідження) : дисертація ...канд. юрид. наук: 12.00.01. Київ, 2013. 198 с.
7. Україна на третьому місці за скаргами на неї у ЄСПЛ. URL: <https://www.pravda.com.ua/news/2020/01/29/7238785> (дата звернення: 27.01.2020).
8. Терлюк І. Історія держави і права України: доновітній час: навч. посіб. Київ: Атіка, 2006. 399 с.

~~~~~ \* \* \* ~~~~~

УДК 321.01:351+342.3

ДОРОНІН І.М., кандидат юридичних наук, доцент, завідувач наукової лабораторії НДІ інформатики і права НАПрН України.  
ORCID: <https://orcid.org/0000-0002-3941-1013>.

## БЕЗПЕКОВА СУТНІСТЬ ФУНКЦІЙ ДЕРЖАВИ

**Анотація.** У статті досліджено проблему визначення сутності функцій держави. Запропоновано розглядати безпеку як основу для розуміння суті функцій. Аргументовано визнання забезпечення національної безпеки основною функцією держави. У цьому аспекті інші функції держави класифікуються залежно від напрямку національної безпеки. Визнання безпекової сутності дає змогу визначити підстави та обсяг державного регулювання при реалізації функцій. Запропоновано критерій для класифікації функцій в залежності від безпекової сутності. Окреслено подальші напрями досліджень щодо класифікації функцій держави.

**Ключові слова:** держава, функції держави, національна безпека, безпека, економічна функція, екологічна функція, державна політика.

**Summary.** The article analyzes the problems of definition of state functions essence. In this context security is considered as an essence of state functions. Author argues that national security is a main function for a state. Other state functions are classified depending on the areas of national security. Security as essence of state functions enables researchers to determine the scopes and limits of state regulation. The classification criteria for state functions were suggested by author. Further directions for research were aimed.

**Keywords:** State, state functions, national security, security, economic function, ecological function, public policy.

**Аннотация.** В статье исследована проблематика определения сути функций государства. Предложено рассматривать безопасность в качестве основы для понимания сути функций государства. Автором аргументировано признание обеспечения национальной безопасности основной функцией государства. В изложенном аспекте другие функции государства классифицируются в зависимости от направлений национальной безопасности. Признание безопасности сущностной основой функций государства в дальнейшем предоставляет возможность определять основания и объем государственного регулирования в зависимости от сущности функции. Предложен критерий для классификации функций в зависимости от указанной сущностной основы. Изложены основные направления для дальнейших научных исследований проблематики классификации функций государства.

**Ключевые слова:** государство, функции государства, национальная безопасность, безопасность, экономическая функция, экологическая функция, государственная политика.

**Постановка проблеми.** Концепція функцій держави, серцевиною якої є виокремлення поняття, а також визначення сутності функцій, доволі тривалий час розглядається у юридичній науці. Різноманітні підходи застосовуються дослідниками щодо визначення таких функцій, їх класифікації, трансформацій та перспектив розвитку (або відмирання). Водночас, на нашу думку, дослідження сутності функцій залишається багато в чому в рамках класового підходу, характерного для науковців радянського періоду. Вбачається, що сутність функцій неможливо розглядати у відриві від розуміння сутності держави. Протягом тривалого часу кожен із дослідників, що зосереджувався на проблематиці функцій держави, ґрунтувався на відповідному сприйнятті суті держави, яка відповідала конкретному історичному періоду.

На нашу думку, доцільно розглядати суть держави, ґрунтуючись на розумінні завдання держави, що полягає у забезпеченні безпеки – окремої людини та суспільства як об'єднання людей. Ідеї, що були свого часу викладені Т. Гоббсом, і які полягають у розумінні того факту, що мета держави – це забезпечення безпеки, а потреба людини в державі зумовлена необхідністю примусу, оскільки безпека не гарантується природнім правом [1, с. 129], залишаються повністю актуальними. Більш того, саме таке розуміння держави відповідає сучасній державі як соціальному інституту. Традиційно держава Т. Гоббса розуміється у негативному аспекті – як вираження необхідного зла. Водночас, саме в ідеї забезпечення безпеки, як мети держави, можливо виокремити підстави та межі державного втручання, оскільки концепт “безпеки” також змінюється.

**Результати аналізу наукових публікацій.** Проблематика функцій держави досліджувалась багатьма науковцями, як радянського періоду, так і сучасними. Характеристику основних підходів до визначення суті функцій буде викладено в основному розділі роботи. Загалом їх можливо розділити наступним чином. По-перше, це розуміння функцій в межах вузько-класового підходу, що характеризувався аксіоматичним викладенням політичних доктрин радянського періоду. Саме таким чином викладали концепцію функцій держави науковці у 1940-50-ті роки (Г.Є. Глезерман, А.І. Денисов, Й.М. Левін, Д.М. Чесноков). У подальшому (у 1960-70-ті роки) підхід було дещо розширено, у т.ч. із поверненням до загального розуміння функцій держави як основних напрямів діяльності, що було традиційним для дореволюційних теоретиків права. Цю точку зору висловили та аргументували М.Й. Байтін, Л.І. Загайнов, А.І. Йориш, Ю.Б. Кравченко, Б.П. Курашвілі, М.І. Піскотін, О.А. Рогачов, П.С. Ромашкін, В.О. Тененбаум, М.В. Черноголовкін та інші. Своєрідними у межах концепцій радянського періоду є наукові погляди на сутність функції держави, висловлені О.П. Глебовим та Л.І. Каском. Починаючи з 1990-х років у правовій науці спостерігається численні спроби модифікації концепції функцій держави, водночас аспекти визначення їх сутності залишаються дослідженими недостатньо.

Останнім часом, проблеми визначення суті функцій держави перебували у полі зору вітчизняних науковців О.О. Джураєвої, М.В. Дзевелюк, О.В. Зайчука, Л.Р. Наливайко та інших.

**Метою статті** є визначення суті функцій сучасної держави, порівняно із відповідними напрацюваннями у сфері національної безпеки, виокремлення дотичних точок та аргументація щодо розуміння безпеки, як суті функції держави, з наступним дослідженням поняття “безпеки”, як підстави для можливих класифікацій функцій та визначення підстав, меж та обсягів державного впливу на суспільні відносини.

**Виклад основного матеріалу.** Як правило в наукових працях традиційним є сприйняття поняття через з'ясування його сутності. Термін “функція” використовується в різних значеннях та різних видах людської діяльності, тому сфера його застосування може виходити за межі правової науки. У суспільних науках, зокрема, у соціології він розглядається передусім у контексті ідей організму.

Досліджуючи проблему структури та функції у примітивному суспільстві, А. Редкліфф-Браун зазначає, що в соціальній науці термін “функція” застосовується за аналогією між соціальним і органічним життям, тобто робиться висновок щодо аналогії між соціальним і біологічним організмом. У фізіології поняття “функція” розглядається як одне із найважливіших разом з поняттями “структури” і “процесу”. Кожен організм має структуру, яку утворюють окремі елементи, що входять до його складу. Процеси, що відбуваються в організмі перебувають у залежності від його структури та підтримуються функціями, що забезпечують ці процеси [2, с. 12-13]. Таким же чином

зазначена аналогія із застосуванням термінології, що характерна для біології провадиться у соціальних науках Її підґрунтя складають роботи Е. Дюркгейма, Г. Спенсера, А. Шеффле та інших. Суспільство розуміється як аналог біологічного організму з певними функціями, що йому притаманні. При цьому кожна функція (а також їх сукупність) забезпечують процеси, які відбуваються в організмі, аналогічно кожна функція суспільства забезпечує його процеси та у сукупності – життєдіяльність. У подальшому подібні ідеї були розвинуті у працях Р. Мертон, Т. Парсонса та інших прихильників функціоналізму, як більш вузького напрямку органіцизму [3, с. 209-211].

Викладені підходи щодо застосування терміну “функція” в соціології можуть бути цілком використані і стосовно функцій держави. Більш того, в останні роки у правовій науці активно використовуються концепції соціологічної науки, у тому числі і класичного функціоналізму. Низка новітніх досліджень функцій держави прямо ґрунтуються на положеннях органіцизму та функціоналізму, запозичуючи не тільки термінологію біології, а і поняття притаманні медичним наукам, що разом із використанням концепцій сучасної політичної філософії (зокрема, Ф. Фукуями), призводить до формулювання так званих теорій “дисфункціональної держави” [4, с. 16-18; 5, с. 18-20, 6. с. 296-297]. Але в соціологічній науці існує і дещо інше сприйняття функцій. Зокрема, Н. Луман сформулював розуміння функції на суто теоретичному рівні. На його думку, поняття функції означає предметний зміст, що виходить за межі голої неперервності самореферентної репродукції (“підтримання постійності”) [7, с. 92]. При цьому окремі функції здійснюють саморегулювання системи, забезпечуючи підтримання динамічної рівноваги. Якщо розуміти державу, як систему, виокремлюючи у ній функції, то фактично вони забезпечують існування та рівновагу всієї системи.

У теорії держави і права складність дослідження функцій держави полягає і у значній мінливості предмету пізнання для дослідника. Існує плуралізм думок щодо розуміння власне суті держави, її виникнення та періодизації. Такі теорії варто розглядати разом із особистістю дослідників, що їх проводять, оскільки розуміння суті держави відповідають історичному періоду життя дослідника, його місця знаходження та стану сучасних йому держав. Так, за підрахунками Т.К. Аляб'євої можливо виділити принаймні 40 теорій та доктрин походження держави [8, с. 6-11, 550-552]. Кожна група дослідників ґрунтувалась на своєму сприйнятті суті держави, іноді виокремлюючи “сучасну” (для них) державу та інші попередні форми у залежності від історичного етапу розвитку. Особливості розуміння суті держави, її властивостей, виникнення та етапів розвитку, відображається і на з'ясуванні суті функцій держави.

Насамперед слід зазначити, що загальне (або класичне) розуміння функцій держави ґрунтується ще на працях російських дореволюційних юристів, погляди яких відповідали поглядам сучасних їм європейських правників. Зокрема, М.М. Коркунов у своєму курсі державного права визначав “функції державного владарювання”, оскільки поняття “держава” та “суспільство” не ототожнювались [9, с. 3-5]. В основі розуміння поняття “держава” знаходиться державне владарювання, тобто предмет дослідження було зміщено від “держави” до “влади”. На цей період часу та в умовах фактичної абсолютної монархії в Російській імперії держава в суспільній свідомості (яка відображалась і у свідомості науковців) не могла розглядатись окремо від монарха. У такому разі функції владарювання (як реалізації державної влади) розуміються цілком у дусі вчення Ш. Монтеск'є внаслідок розподілу влади на виконавчу, законодавчу та судову. Тобто мова йде про законодавчу, виконавчу та судову функції державного владарювання [9, с. 369-374].

Позиція М.М. Коркунова безперечно сформована під впливом праць німецьких юристів щодо організації державної влади. Так, Г. Єллінек поняття “функції” розглядає як завдання і функції загалом держави, а також як функції окремих державних органів. За таких умов окремі галузі управління – “справи” іноземні, військові, внутрішні, фінанси та юстиція розуміються не як функції, а як завдання держави. У свою чергу функції пропонується розподілити на матеріальні (як основні напрямки державної діяльності) та формальні (функції певних груп органів держави), уся ж діяльність держави має бути спрямована на досягнення її цілей [10, с. 595]. У даному випадку можливо відзначити окрему правосуб’єктність держави в розумінні Г. Єллінека. Така точка зору є більш характерною для науковців тих шкіл, що засновані на західній традиції права. Наприклад, М. Ван Кревельд, характеризуючи загальне поняття “держава”, визначав державу як сутність, що має окрему правосуб’єктність [11, с. 1, 53, 57].

Переосмислення концептуальних поглядів німецьких юристів у російській дореволюційній науці призвело до виокремлення однієї функції. Або ж якщо говорити точніше, то мова йде про фактичне об’єднання усіх функцій в одну, оскільки в Російській імперії фактично до її розпаду влада монарха об’єднувала у собі усі функції та усі види влади [12, т. 1, с. 118]. В умовах абсолютної монархії інакше організація влади в державі розглядатись не могла. Саме тому, наприклад, Ф. Мартенс вважав, що державна влада єдина та неділима, водночас має певні визначені функції. Тому про розподіл влади мова не йшла у принципі. За таких умов певні функції, що їх має держава, слід розуміти як обов’язки, що на неї (владу) покладені, а також ті дії, які вона повинна здійснювати в різних галузях державного життя [13, с. 49, 51]. Більш того, окремі юристи вважали, що теорія Ш. Монтеск’є не витримала теоретичної і практичної критики, а за умови російських правових реалій та особливостей національного розвитку, функції держави слід розуміти лише як функції верховної влади, а монарх, що її має, об’єднує в своїй діяльності усі ті напрямки, які Ш. Монтеск’є вважав відокремленими [14, с. 128-129].

У радянській правовій науці інтерес до визначення функцій держави виник у 1950-ті роки. До цього часу ця проблематика була мало досліджена внаслідок певної ідеологічної зашореності. Річ у тім, що безпосередньо у працях К. Маркса та “класиків” марксизму-ленінізму питання визначення функцій держави майже не підіймалось, оскільки буржуазна держава розглядалась лише як суб’єкт пригнічення та поневолення. Більш того, свого часу з цього приводу публічно свою точку зору висказав Й. Сталін. Він визначав у виступах, що існує усього дві функції держави – функція пригноблення (внутрішня) і захисту території (зовнішня). Враховуючи політичну ситуацію в СРСР за часів сталінізму, інші формулювання та сприйняття функцій держави були неможливі, тому варто погодитись з точкою зору В.О. Тененбаума щодо тривалої обмеженості розуміння функцій держави політичною позицією Й. Сталіна [15, с. 135-138].

Таким чином, будь-яка наукова дискусія з приводу функцій держави фактично була неможлива, окрім аксіоматичного викладення відповідних ідеологічних догм та постулатів [16 – 19]. Тому, аналізуючи стан розробки проблеми, М.І. Піскотін свого часу прийшов до висновку, що до кінця 1950-х років у радянській правовій науці функції держави розумілись лише у розрізі директив партійного керівництва [20, с. 89]. На початку розробки зазначеної проблематики розуміння функцій держави ґрунтувалось на визначеннях, що наводились Г. Єллінеком, а саме у тому, що функціями держави вважались основні напрями його діяльності. Зрозуміло, що зазвичай до цього додавалось посилення на відображення класової сутності держави у таких основних напрямках [21, с. 5; 22, с. 190-191; 23, с. 75]. З тими чи іншими модифікаціями це сутнісне розуміння функцій залишалось незмінним протягом доволі тривалого часу.

Більш того за винятком посилань на класову сутність та її відображення функції держави викладаються як напрями її діяльності і у більшості підручників та навчальних посібників з теорії держави і права до цього часу.

Певні уточнення та обережні зміни у підходах спостерігаються лише останнім часом. Зокрема, це стосується відображення у визначенні поняття функцій держави, як діяльності з управління суспільством, цілей та соціального призначення держави [24, с. 97; 25, с. 100-101, 105]. І.А. Іванніков, досліджуючи проблематику функцій держави, особливо підкреслював одночасне розуміння функцій як напрямів діяльності держави та її основних обов'язків, в яких виражаються та конкретизуються її класова сутність та соціальне призначення [26, с. 122]. Подібні визначення ілюструють усталену в правовій науці кінця ХХ – початку ХХІ сторіччя тенденцію до намагання поєднання різних (іноді протилежних за змістом та ідеологічною основою) концепцій, у т.ч. із залишенням у наукових дефініціях класового характеру, як складової, з одночасним ужиттям термінології (як додатковою так і заміною) “загальнолюдянської” сутності.

Слід зазначити, що в окремих наукових працях радянського періоду було зроблено спроби вийти за межі усталених уявлень та більш обґрунтовано використати поняття функцій держави. Так в окремих роботах вчені намагалися застосувати елементи системного підходу. В.О. Тененбаум запропонував досліджувати державу, як систему певних категорій, а функції держави входили до такої системи [15, с. 18-19, 134-135]. Розуміння функції у такому випадку відповідало визначенню, запропонованому М.І. Піскотінім, для “основних функцій” держави, як таких видів діяльності, потреба у здійсненні яких породжує необхідність існування держави, вони виражають найбільш істотні риси держави, її соціальну природу та складають загальні напрями діяльності, що спрямовані на виконання основних (корінних) завдань держави на відповідному етапі розвитку [20, с. 90]. Але зазначені конструкції застосовувались до соціалістичної держави, оскільки антагоністична сутність держав різного типу закріплювалась на рівні ідеологічних догм. Для капіталістичної держави основним вважалось завдання придушення, оскільки саме це на думку класиків марксизму-ленізму складало її сутність [27, с. 67-69].

Оскільки позиція про відображення у суті функцій суті самої держави стосувалась обох типів держави, з 1970-х років у радянській правовій науці відбувався активний пошук додаткової аргументації. Зокрема, це стосувалось дослідження аспектів життєдіяльності держави, пошук, виокремлення та визначення головної (сутнісної) складової діяльності держави, що відповідає її корінним завданням. Зокрема, О.П. Глебов запропонував розглядати проблематику функцій держави у контексті сутнісного елементу державної функції [28, с. 12]. На той період часу таким сутнісним елементом можливо було вважати соціально-класове призначення держави. Природно, що розуміння держави у межах класового підходу неодмінно призводило до висновку про наявність низки істотних моментів. По-перше, соціально-класове призначення держави проявляється у тому, що вона виражає інтереси панівного класу (хоча у випадку соціалістичної держави неодмінно виникає протиріччя, яке пропонується вирішувати з урахуванням розуміння тимчасового характеру держави у період переходу до комунізму). По-друге, соціально-класове призначення держави визначається як досить умовне за своїм змістом, оскільки “панівний клас” може складатись із різних соціальних груп, інтереси яких можуть не співпадати. Для сучасного дослідника є очевидним, що у випадку соціалістичної держави її фактичний устрій відрізняється від декларованого на політичному рівні та навіть від законодавчо встановленого. І по-третє, “соціально-класове призначення”, як сутнісний елемент, визначає характер інших елементів функції [28, с. 12].

У такому випадку знову ж таки було піднято питання про існування “головної функції” держави. На думку О.П. Глебова це так звана “цільова” функція, яку можливо виокремити від багатьох інших функцій, що є функціями-задачами. Визначаючи ціль держави, можливо визначити цільову функцію, а потім і окремі функції-завдання.

У подальшому точка зору щодо головної та цільової функції знайшла своє відображення у концепції “генеральної функції”, яку запропонував Л.І. Спиридонов [29, с. 47]. Водночас, О.О. Джураєва, визнаючи можливість виокремлення генеральної функції, вважає за можливе розглядати її як поняття, що охоплює окремі складові, а саме як “всеохоплюючу категорію”, яка “розкриває призначення держави відносно громадянського суспільства через реалізацію внутрішніх та зовнішніх функцій” [30, с. 110]. Існування такої генеральної функції зумовлено певними категоріями (“загальних справ”), реалізація яких забезпечує об’єктивні умови людського існування [31, с. 12].

Таким чином, існування однієї основної (цільової, головної, генеральної) функції, в якій відображається саме призначення держави, науково визначено. Водночас, питання щодо її змісту залишається відкритим. Слід зазначити, що висновок про існування однієї основної функції поділяється далеко не усіма дослідниками. Так, Л.Р. Наливайко у своїй ґрунтовній роботі, присвяченій теоретико-правовій моделі державного ладу, визначає п’ять “об’єктних” функцій Української держави – політичну, економічну, соціальну, екологічну та культурну, не виокремлюючи одну з них як основну [32, с. 402-403]. Свого часу М.В. Чернооголовкін також виокремлював численні основні функції держави [21, с. 131]. Позиція щодо наявності низки основних функцій є достатньо дискусійною і зумовлює постановку відповідних питань.

Зокрема, зважаючи на задекларовану наявність однієї головної (основної, генеральної) функції держави, будь-яка функція із тих, що розглядаються, може бути визнана основною чи допоміжною. Класифікація за принципом “основні та неосновні”, викликатиме і необхідність у створенні свого роду ієрархії функцій, як поділу основних на неосновні, або ж визначення частини неосновних як допоміжних. За таких умов термінологічне виокремлення “основної” функції втрачає сенс. Якщо розуміти сутнісну функцію як генеральну для інших, то відповідна систематизація зумовлюється необхідністю її розподілу на елементи за напрямками.

Як правило, систематизація функцій держави ускладнена низкою факторів.

Перелік функцій держави не є визначеним, класифікованим, а також – усталеним внаслідок складнощів із визначенням суті держави. Якщо повертатись до поглядів, висловлених класиками марксизму-ленінізму та їх прихильниками, то вони вважали чітко визначеною лише функцію придушення (пригнічення), тобто здійснення примусу в інтересах “панівного класу”. Стосовно інших функцій позиція дослідників радянського періоду характеризується переліченням досить великої їх кількості. Особливо це стосувалось історичного періоду так званого “розвиненого соціалізму” (з 1960-х років), оскільки до цього часу вважалося, що в СРСР ще здійснюється класова боротьба і, отже, зберігається наявність функції, змістом якої є придушення спротиву залишків експлуататорських класів. Зазначений стан речей ускладнюється і множинністю критеріїв для класифікацій.

Так, більшість дослідників вважає беззаперечним поділ функцій держави на внутрішні та зовнішні. Критерієм поділу в такому разі є спрямованість функції за межі території держави. Тобто сутність зовнішньої функції має полягати у тому, що вона будь-яким чином розповсюджується на інші держави. Але можливість визначення суті зовнішньої функції є доволі проблематичним. Складнощі з цього приводу виникали ще при визначенні суті зовнішньої функції у минулому сторіччі. Більш того, окремі

формулювання назв зовнішніх функцій, що були запропоновані ще за часів СРСР і використовуються у науковій літературі до цього часу, є досить розпливчастими, наприклад, це стосується функції “забезпечення миру та підтримки світового правопорядку” [33, с. 134]. Річ у тім, що, як правило, така функція визнається одночасно із наявністю у держави оборонної функції, але у випадку відсічі агресії проти держави виникає питання у самому змісті та окремих складових функції “забезпечення миру” на власній території. До речі, дослідниками функція оборони держави розглядається як зовнішня з аргументацією тим фактом, що загроза виходить з-поза меж держави [34, с. 120-121]. Але у такому разі критерій належності функції до внутрішніх та зовнішніх доволі хиткий, оскільки належність функції визначається не за територіальною ознакою, а чомусь за характером “загрози”.

Окрім цього, враховуючи глобалізацію, як сучасний і постійний фактор впливу на державу, певні “традиційні” функції також можуть мати одночасно і зовнішній, і внутрішній характер. Критикуючи поділ функцій держави на зовнішні та внутрішні, М.В. Дзевелюк звернула увагу на той факт, що в умовах сучасного глобалізованого світу неможливо чітко визначити суто внутрішні функції [35, с. 71].

Погоджуючись із дослідницею, можливо лише зауважити, що більшою мірою це стосується саме зовнішніх функцій, враховуючи складність їх виокремлення. Зокрема, якщо взагалі виділяти державну функцію забезпечення миру, то рівною мірою вона може стосуватись як внутрішньої, так і зовнішньої політики. За таких умов безпосередньо до зовнішньої функції належить лише здійснення діяльності з підтримання зовнішніх відносин з іншими державами, що термінологічно розглядається як “дипломатична” функція, (зовнішньополітична або ж “функція зовнішніх відносин”) [36, с. 45]. “Зовнішньоекономічна” функція держави є атрибутом держави соціалістичного типу з жорстким обмеженням зовнішньої торгівлі, а тому може розглядатись лише як складова зовнішньополітичної функції.

Слід також зазначити, що практично безмежним для будь-яких спроб класифікації залишається критерій поділу функцій держави на підставі визначення об’єкту для державного впливу. Наразі неможливо навіть приблизно перелічити усі функції, існування яких запропоновано багатьма дослідниками, що зосереджували свою увагу на певній одній визначеній функції, формулювання назви якої ними ж і пропонувалось. Більш того, сутність однієї і тієї ж за назвою функції може визначатись по-різному, при цьому доволі часто одна окрема функція визначається як складне явище, що охоплює багато різноманітних складових. Водночас, Л.Р. Наливайко вважає, що можливо систематизувати функції за об’єктами (сферами) діяльності. До числа об’єктних у сучасній українській державі, як вже зазначалось вище, належить політична, економічна, соціальна, екологічна та культурна [32, с. 402-403]. Кожна з функцій є нормативно визначеними конкретними напрямками і видами діяльності держави.

На наш погляд можливо дещо змінити підходи взявши за основу класифікації безпекову сутність держави, а відтоді – і безпекову сутність її функцій. Тим більше, що такий підхід відповідає загальним поглядам стосовно засад широкої класифікації об’єктів на два класи, один з яких точно не є іншим [37, с. 18]. Тому пропонується поєднати підхід до критерію класифікації функцій держави із виокремленням складових (напрямів) національної безпеки.

Так, функція оборони держави ототожнюється із військовим захистом держави від нападу зовні, а її складові розглядаються через призму військових (власне військових, військово-політичних, або забезпечення військової політики) заходів [34, с. 120; 38, с. 39]. Існують і дещо інші точки зору. Наприклад, російський науковець Д.В. Пожарський

обґрунтовує точку зору щодо існування охоронної функції держави, що об'єднує у собі публічно-владну діяльність з метою нейтралізації загроз суспільству [39, с. 142]. При цьому власне це діяльність з охорони досить великої кількості об'єктів, а зазначене формулювання розширює зміст функції, практично об'єднуючи у собі всі складові функції оборони держави.

У науковій літературі до змісту функції оборони запропоновано віднести: 1) діяльність по безпосередньому збройному захисту; 2) удосконалення матеріальних та інших основ військової організації; 3) попередження і припинення підіривної діяльності; 4) вдосконалення засобів цивільної оборони [40, с. 67].

Доволі часто функція оборони поєднується з функцією забезпечення національної безпеки, іноді вживаючи їх як синоніми, або елементи одного поняття. Разом із цим, Л.Р. Наливайко розглядає національну безпеку, як складову політичної функції (у запропонованій нею системі з п'яти об'єктних функцій). Зміст функції визначається як “нормативно-визначені напрями та види діяльності” держави “з регулювання сфери політичних відносин, вироблення й реалізації внутрішньої та зовнішньої політики, створення умов та інститутів для розвитку народовладдя й політичної стабільності та забезпечення національної безпеки з метою формування громадянського суспільства” [32, с. 402]. Тобто “національна безпека” розуміється як завдання поряд із розвитком народовладдя, політичною стабільністю, а метою діяльності є формування громадянського суспільства.

Зазначений підхід є прийнятним на рівні теоретичної конструкції. Але, як показує аналіз чинних законодавчих актів, що є наслідком втілення певних наукових підходів, формування політики в Україні має відбуватись наступним шляхом. Статтею 85 Конституції України визначення засад внутрішньої та зовнішньої політики віднесено до компетенції Верховної Ради України. Здійснення ж внутрішньої і зовнішньої політики відповідно до приписів ст. 116 Конституції України покладено на Кабінет Міністрів України.

Якщо аналізувати зміст спеціального законодавчого акту – Закону України “Про засади внутрішньої і зовнішньої політики” від 01 липня 2010 р., то можливо прийти до висновку щодо законодавчої універсалізації державної діяльності у формі здійснення внутрішньої та зовнішньої політики. Стаття 1 цього законодавчого акту встановлює, що засади внутрішньої та зовнішньої політики визначають принципи та пріоритети державної політики у відповідних сферах [41]. Таким чином під узагальненим терміном “внутрішня та зовнішня політика” можливо розуміти усю діяльність держави, яка може бути розподілена за відповідними сферами.

Преамбула Закону України “Про засади внутрішньої і зовнішньої політики” містить перелік сфер діяльності, тобто визначає предметне поле для діяльності держави. До цих сфер належать: – розбудова державності, – розвиток місцевого самоврядування та стимулювання розвитку регіонів, – формування інститутів громадянського суспільства, – національна безпека і оборона, – економічна, – соціальна, – гуманітарна, – екологічна сфера та сфера техногенної безпеки. Окрім цього, згадується “зовнішня політика”, що за буквальним тлумаченням тексту преамбули також може бути визначена як сфера [41].

Повертаючись до запропонованого Л.Р. Наливайко змісту політичної функції Української держави, можливо помітити що у трактуванні вироблення і реалізації внутрішньої та зовнішньої політики, мова йде фактично про генералізацію окремої (у даному разі – політичної) функції, що має реальні підстави вважатися основною для держави.

На нашу думку, слід звернути увагу на дослідження принципової можливості систематизації функцій держави. Аналізуючи пропозиції Л.І. Каска щодо доцільності застосування до пізнання у науці держави і права концепції та понятійного апарату загальної теорії систем [42, с. 31], варто визначитись яким саме чином варто розуміти систему. У теорії систем, її розуміють як сукупність закономірно пов'язаних в єдине ціле елементів, що має властивості, що відсутні у елементів, які її утворюють [43, с. 6]. Особливо важливим є розуміння суті системи саме як сукупності елементів (об'єктів) разом із зв'язками (відносинами) між ними та їх атрибутами (властивостями) [44, с. 252]. Критично важливим є розуміння рівнозначності сприйняття елементів, зв'язків та атрибутів.

Отже, визначаючи функції держави, як системи, необхідно з'ясувати окрім сукупності елементів, що її складають, також їх зв'язки та атрибути. Оскільки, держава також може розумітись як система, доцільно також визначити її мету, у такому разі мова може йти про формулювання мети системи. Якщо позбутись політично забарвленої ідеології, мета держави (а по суті головна причина її існування) має бути визначена як забезпечення безпеки людини. Похідним від цього є досить широкий комплекс складових безпеки, як універсального поняття, що проявляється у формулюванні її видів з виокремленням відповідних об'єктів, у тому числі тих інститутів, що забезпечують безпеку людини. Такий підхід базується на ідеях, що були свого часу закладені Т. Гоббсом, який прямо зазначав, що мета держави в основному це забезпечення безпеки, а потреба людини в державі зумовлена необхідністю примусу, оскільки безпека не гарантується природнім правом [1, с. 129-130].

З'ясувавши мету держави, можливо визначити її елементи (органи), атрибути (дворівневі функції – загалом держави та її органів) та зв'язки між ними, що мають досить складний характер.

На нашу думку, забезпечення національної безпеки має особливе місце в зазначеній системі. Спроби визначення місця забезпечення національної безпеки у системі функцій держави мали місце. Так, О.В. Лемак запропонував розглядати забезпечення національної безпеки, як функцію держави. Щодо сутності функції дослідник зазначив, що вона “є невід'ємною від основних напрямків діяльності держави та полягає у забезпеченні безпеки відповідних національних інтересів (цінностей) у військово-силовій, екологічній, економічній, політичній, інформаційній сферах або об'єктів захисту, відповідно, територіальної, екологічної, економічної, політичної та інформаційної безпеки держави за умови виникнення негативних тенденцій до створення потенційних або реальних загроз національним інтересам” [45, с. 67]. Отже, у такому визначенні сутністю функції оголошується забезпечення безпеки у певних сферах (усього наводиться п'ять) та щодо об'єктів захисту (п'ять об'єктів, що відповідають п'яти складовим безпеки за видами об'єктів). Зазначена кількість видів безпеки (за термінологією, вжитою О.В. Лемаком – “об'єктів захисту”) зумовлена підходами, що закладено у Законі України “Про основи національної безпеки України” від 19 червня 2003 р., перша редакція якого визначає 9 сфер існування загроз національним інтересам і національній безпеці, а також відповідні 9 сфер напрямів державної політики з питань національної безпеки [46].

Таким чином, вірно визначивши загальний характер суті безпеки на рівні суспільства (як безпеки національної) та з'ясувавши її забезпечення на рівні функцій держави (з чим варто погодитись) дослідник утримався від її визначення як основної. На нашу думку, такий характер функції забезпечення національної безпеки не може дозволити розглядати її інакше аніж головна (основна, генеральна) функція держави.

В іншому разі втрачається загальний характер поняття “національна безпека”, що пов’язується із забезпеченням держави як соціального явища (у тому числі суспільства та людини). Саме в основній функції забезпечення національної безпеки і полягає сутність держави, як соціального інституту.

Отже, при конкретизації окремих функцій слід зважати і на визначення окремих складових національної безпеки, а враховуючи, що метою держави є безпека, можливо провести своєрідну ревізію переліку запропонованих у науці окремих функцій. Визначаючи функції держави термінологічно, можливо відійти від певних формулювань, проаналізувавши окремі з них із врахуванням висловлених пропозицій щодо їх суті.

Отже, функції можливо конкретизувати і кореспондувати із напрямками безпеки. Як вже було зазначено, навряд чи можливо підрахувати усі пропозиції стосовно визначення функцій. Але основними з них (або об’єктними за термінологією, запропонованою Л.Р. Наливайко) пропонується вважати політичну, економічну, соціальну, екологічну та культурну. На нашу думку кожна з них по суті може корелюватись із уявленням про той чи інший вид безпеки.

Загальний підхід до співвідношення видів безпеки із відповідними функціями у межах розуміння національної безпеки, як основи, може бути викладено у наступній таблиці.

| <b>Національна безпека</b><br>(як основа) |                                                                                                                                                                                                           |
|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>Найменування напрямку безпеки</i>      | <i>Найменування функцій</i><br>(з відповідними варіантами назви, що запропоновані у літературі)                                                                                                           |
| Державна безпека                          | Політична функція<br>(функція забезпечення державної безпеки)<br>(функція розвідки)<br>(контррозвідувальна функція)                                                                                       |
| Воєнна безпека                            | Функція оборони                                                                                                                                                                                           |
| Економічна безпека                        | Економічна функція<br>(фінансова функція)<br>(фіскальна функція)<br>(митна функція)                                                                                                                       |
| Соціальна (громадська, суспільна) безпека | Правоохоронна функція<br>(функція охорони громадського порядку)<br>(функція боротьби зі злочинністю)<br>Соціальна функція<br>(функція соціального захисту)<br>(функція забезпечення продовольчої безпеки) |
| Екологічна безпека                        | Екологічна функція<br>(функція забезпечення екологічної безпеки)                                                                                                                                          |
| Інформаційна безпека                      | Інформаційна функція<br>(комунікативна функція)<br>(ідеологічна функція)<br>(культурно-виховна функція)                                                                                                   |

Як уже було зазначено вище, науковцями в останні 40 років було запропоновано значну кількість найменувань для окремих функцій держави. Загальні підходи при цьому

дозволяють говорити про надмірну їх деталізацію, а отже і до невиправданого збільшення обсягу державного регулювання щодо тих чи інших сфер суспільного життя.

Запропонований вище підхід стосовно безпекової сутності функцій держави може розглядатись щодо окремих визначених вище наступним чином.

Екологічна функція держави, що в літературі видається складною і багатоаспектною, по суті розуміється як діяльність із забезпечення (раціонального) природокористування, охорони навколишнього природного середовища та екологічної безпеки (із можливістю розгляду інших похідних властивостей) [47, с. 9; 48, с. 23]. Якщо зважати, що екологічною безпекою по суті є стан захищеності від загроз, які є наслідком у тому числі антропогенної діяльності [49, с. 76], то державний вплив у вигляді забезпечення раціонального природокористування та охорони навколишнього природного середовища (як складових екологічної функції) є похідним від необхідності забезпечення екологічної безпеки.

Щодо економічної функції слід зазначити, що у сучасній науковій літературі найбільш детально питання її визначення досліджувались О.М. Лоцихіним. У загальному вигляді ним пропонується розуміти економічну функцію у контексті вироблення та координації стратегічних напрямів розвитку економіки країни в найбільш оптимальному режимі, надаючи їй визначення як основного, постійного напрямку і виду “діяльності держави в економічній і суміжних з нею сферах, зумовленої об’єктивними потребами розвитку ринкових відносин” [50, с. 4, 19]. Зазначене визначення є цілком вірним, воно відображає зміну місця і ролі держави в регуляції суспільних на етапі пострадянських трансформацій. Але потребою у діяльності держави в економічній сфері має бути саме забезпечення безпеки для всього суспільства. Отже, можливо вести мову про відповідність економічної функції потребам економічної безпеки, якщо розуміти останню як здатність економіки забезпечувати “підтримувати послідовну реалізацію національно-державних інтересів, стійку дієздатність господарських суб’єктів, нормальні умови життєдіяльності населення” [51, с. 11]. Обумовленість впливу держави на економіку внаслідок реалізації економічної функції може бути зумовлено потребами у забезпеченні безпеки іншого виду. Так, наприклад, потреба в обороні держави (у широкому розумінні) може зумовлювати необхідність існування державної форми власності стосовно певного виду об’єктів – космічної галузі, ядерної енергетики, загальнодержавного транспорту [50, с. 20].

У контексті реалізації економічної функції можливо виокремити певні напрями забезпечення безпеки. Зокрема, О.О. Бригінець, досліджуючи питання забезпечення фінансової безпеки України, як складової економічної безпеки, надає їй визначення як стану, “за якого забезпечується належне функціонування усіх суб’єктів фінансових правовідносин у державі, що характеризується стійкістю до будь-яких реальних чи потенційних, зовнішніх та внутрішніх негативних впливів, який спроможний забезпечити ефективне функціонування національної фінансової системи, а також її поступальний розвиток” [52, с. 139]. Отже, економічна безпека, як вид безпеки, може розподілятися на підвиди, так само як і її реалізація може стосуватись різних сфер національної економіки, але потреба в державному впливі має бути зумовлена потребами забезпечення безпеки. Цей аргумент може бути застосований і щодо окремих функцій в контексті відповідних видів безпеки, які сукупно складають національну безпеку.

### **Висновки.**

Викладений вище аналіз та надані аргументи дозволяють прийти до наступного:

1. Пошук критеріїв для систематизації функцій держави має ґрунтуватись на розумінні суті держави, за таких умов безумовним є існування її основної (сутнісної, генеральної) функції. Беручи до уваги мету держави, що полягає у забезпеченні безпеки

для кожного індивіда та суспільства, і є умовою виникнення цього інституту (у відриві від суверена), саме забезпечення національної безпеки повинно розглядатись як основна функція держави.

2. За умови викладеного вище, необхідно визнати відсутність вагомих підстав для виокремлення тих чи інших функцій держави, окрім тих, що у своїй сутності є функціями забезпечення окремих видів безпеки. Найменування конкретної функції може відрізнятись. Крім цього, цілком можливо вести мову про встановлення підфункцій (субфункцій), або виокремлювати інші структурні елементи, що можуть утворювати певну ієрархію. Але безпекова сутність має розглядатись як основа для розуміння суті функції держави.

3. Саме безпекова основа є підставою, умовою та критерієм для обсягів державного регулювання, тобто втручання держави в суспільне життя. Безпекова сутність в такому розумінні може вважатись і гарантією від надмірного втручання.

### Використана література

1. Гоббс Т. Левиафан, или материя, форма и власть государства церковного и гражданского. Соч. в 2-х т. Москва: Мысль, 1991. Т. 2. С. 3-545.
2. Radcliffe-Brown A. Structure and Function in Primitive Society. Glencoe: The Free Press, 1952. 228 p.
3. Коллинз Р. Четыре социологических традиции. Москва: Территория будущего, 2009. 320 с.
4. Фукуяма Ф. Сильное государство. Управление и мировой порядок в XXI веке. Москва: АСТ, 2006. 220 с.
5. Понкин И.В. Дисфункциональное государство и дисфункциональное государственное управление. *Право и образование*. 2015. № 3. С. 17-28.
6. Masloch P. The Management of Dysfunctional States in the Aspect of Contemporary Threats of Illegal Immigration. *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*. 2018, Vol. 128. P. 295-305.
7. Луман Н. Социальные системы. Очерк общей теории. Санкт-Петербург: Наука, 2007. 644 с.
8. Алябьева Т.К. Теории и общественная практика происхождения государства. Москва: Изд-во МГОУ, 2012. 556 с.
9. Коркунов Н.М. Русское государственное право: в 2-х т. Санкт-Петербург, 1909. Т. 1. 630 с.
10. Jellinek G. Allgemeine Staatslehre. Berlin: Verlag von O.Häring, 1914. 838 s.
11. Van Creveld M. The Rise and Decline of the State. Cambridge: Cambridge University Press, 1999. 448 p.
12. Куплеваский Н.О. Русское государственное право: в 2-х т. 2-е изд. Харьков, Изд-во Дредера, 1902. Т. 1. 354 с.
13. Мартенс Ф.Ф. Лекции по государственному праву. Санкт-Петербург: Императорское училище правоведения, 1892. 276 с.
14. Градовский А.Д. Начала русского государственного права: 2-е изд. Ч. 1. Санкт-Петербург, 1907. 580 с.
15. Тененбаум В.О. Государство: система категорий. Саратов: Изд-во СГУ. 1971. 214 с.
16. Денисов А.И. Теория государства и права: учебник. Москва: Юрид. изд-во МЮ СССР, 1948. 532 с.
17. Чесноков Д.И. Советское социалистическое государство. Москва: Госполитиздат, 1952. 632 с.
18. Глезерман Г. Советское социалистическое государство. Москва: Молодая гвардия, 1953. 80 с.
19. Разин В.И. Марксистско-ленинское учение о государстве. Москва: Политиздат, 1966. 48 с.

20. Пискотин М.И. К вопросу о функциях советского государства в современный период. *Советское государство и право*. 1958. № 1. С 89-100.
21. Черноголовкин Н.В. Теория функций социалистического государства. Москва: Юридическая литература, 1970. 215 с.
22. Байтин М.И. Сущность и основные функции социалистического государства. Саратов: Изд-во СГУ, 1979. 302 с.
23. Теория государства и права; под ред. К.А.Мокичева. Москва: Юридическая литература, 1965. 519 с.
24. Мелехин А.В. Теория государства и права: учебник. Москва: Маркет-ДС, 2007. 640 с.
25. Беляева Ю.Н. О социальных функциях государства. *Журнал российского права*. 2016. № 1. С. 99-106.
26. Иванников И.А. Актуальные проблемы теории государства и права: учеб. пособие. Москва: Юрлитинформ, 2009. 343 с.
27. Туманов В.А. О классовой сущности и внутренних функциях капиталистического государства. *Правоведение*. 1966. № 7. С. 60-69.
28. Глебов А.П. Проблемы структуры функций государства: автореф. дис. ...канд. юрид. наук. Москва, 1974. 19 с.
29. Спиридонов Л.И. Теория государства и права: учебник. Москва: Фирма "Гардарика", 1996. 300 с.
30. Джураєва О.О. Генеральна функція держави. *Актуальні проблеми держави і права*. 2004. Вип. 22. С. 107-111.
31. Джураєва О.О. Функції сучасної держави: автореф. дис. ...канд. юрид. наук. Одеса, 2006. 20 с.
32. Наливайко Л.Р. Державний лад України: теоретико-правова модель: монографія. Харків: Право, 2009. 600 с.
33. Скакун О.Ф. Теорія держави і права: підручник. Київ: Правова єдність, 2010. 525 с.
34. Євенко Д.В. Функція оборони у системі функцій держави: гносеологічні підходи. *Науковий вісник Академії муніципального управління. Серія: Право*. 2012. Вип. 1. С. 118-121.
35. Дзевелюк М.В. Традиції та новації в розвитку функцій сучасної держави: дис. ...канд. юрид. наук. Одеса, 2017. 209 с.
36. Андрусенко О.М. До питання про зовнішні функції сучасної держави. *Наукові записки Національного університету "Києво-Могилянська академія". Юридичні науки*. 2006. Т. 53. С. 43-46.
37. Розова С.С. Классификационная проблема в современной науке. Новосибирск: Наука, 1986. 223 с.
38. Щербюк Н., Щербюк М. Особливості та шляхи реалізації функції оборони держави. *Історико-правовий часопис*. 2015. № 2. С. 36-40.
39. Пожарский Д.В. Охранительная функция государства (теоретико-методологические проблемы): дис. ...докт. юрид. наук. Москва, 2014. 418 с.
40. Рогачев А.А. Внешние функции государства социалистического типа. Москва: Изд-во МГУ, 1986. 96 с.
41. Про засади внутрішньої і зовнішньої політики: Закон України від 01.07.10 р. № 2411-VI. Станом на 08.07.18 р. URL: <https://zakon.rada.gov.ua/laws/show/2411-17> (дата звернення 30.12.2019).
42. Каск Л.И. Системный подход в познании государства и права. *Правоведение*. 1977. № 4. С. 31-40.
43. Пьянков В.А., Липенков А.Д. Общая теория систем и системный анализ: учеб. пособ. Челябинск: Издательский центр ЮУрГУ, 2013. 104 с.
44. Холл А.Д., Фейджин Р.Е. Определение понятия системы/ пер. с англ. *Исследования по общей теории систем*; общ. ред. В.Н. Садовский и Э.Г. Юдин. Москва: Прогресс, 1969. С. 252-282.

45. Лемак О.В. Забезпечення національної безпеки як функція держави. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2016. Вип. 38. Т. 2. С. 64-67.
46. Про основи національної безпеки України: Закон України від 19.06.03 р. № 964-IV. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351.
47. Волинець В. Екологічна функція в системі функцій сучасної держави: проблеми правового забезпечення в Україні. *Юридична Україна*. 2012. № 11. С. 4-11.
48. Гиззатуллин Р.Х. Экологическая функция государства: теория и практика реализации: автореф. дис. ...докт. юрид. наук. Москва, 2014. 56 с.
49. Качинський А.Б., Єгоров Ю.В. Екологічна безпека України: системні принципи та методи її формалізації. *Національна безпека: український вимір*. 2009. № 4. С. 71-79.
50. Лощихін О.М. Теоретико-правові характеристики економічної функції сучасної держави: автореф. дис. ...докт. юрид. наук. Київ, 2010. 32 с.
51. Економічна безпека держави: сутність та напрями формування: монографія / Л.С. Шевченко, О.А. Гриценко, С.М. Макуха та ін.; ред. Л.С. Шевченко. Харків: Право, 2009. 312 с.
52. Бригінець О.О. Правове забезпечення фінансової безпеки України: дис. ...докт. юрид. наук. Ірпінь, 2017. 464 с.

~~~~~ \* \* \* ~~~~~

УДК 321.011:65.012.8

СОЛОДКА О.М., кандидат юридичних наук, с.н.с., докторант НА СБ України.
ORCID: <https://orcid.org/0000-0002-1799-0712>.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ ДЕРЖАВИ: ПРАВОВИЙ ДИСКУРС

Анотація. У статті досліджено поняття “інформаційний суверенітет”, його складові та сучасні підходи до розуміння та забезпечення з проекцією на інформаційний простір України. За результатами проведеного дослідження встановлено, що забезпечення інформаційного суверенітету держави вимагає дотримання балансу між правом на інформацію та вимогами щодо обмежень в цілях забезпечення національної безпеки держави, між правом особи на приватність комунікацій та забезпеченням цифрового суверенітету держави.

Ключові слова: інформаційний суверенітет, цифровий суверенітет, інформаційний простір, захист інформаційного простору України.

Summary. The article explores the concept of “information sovereignty”, its components and modern approaches to its comprehension and providing with projection on the information space of Ukraine. According to the results of the research, it was found that ensuring the state's information sovereignty requires balancing the right to information and the requirements for restrictions in order to ensure the national security of the state, between the right of a person to privacy of communications and ensuring the state's digital sovereignty.

Keywords: information sovereignty, digital sovereignty, information space, protection of information space of Ukraine.

Аннотация. В статье проанализированы исследования понятия “информационный суверенитет”, его составляющие и подходы к пониманию и обеспечению с проекцией на информационное пространство Украины. По результатам проведенного исследования установлено, что обеспечение информационного суверенитета государства требует удержания баланса между правом на информацию и требованиями относительно ограничений в целях обеспечения национальной безопасности государства, между правом человека на приватность коммуникаций и обеспечением цифрового суверенитета государства.

Ключевые слова: информационный суверенитет, цифровой суверенитет, информационное пространство, защита информационного пространства Украины.

Постановка проблеми. В умовах розвитку інформаційного суспільства, глобалізації інформаційних процесів, формування глобального інформаційного простору, швидкого зростання світового ринку інформації, розвитку інформаційних технологій, засобів обробки інформації, інформаційних послуг та їх впливу на забезпечення національної та міжнародної безпеки на перший план виходить інформаційна складова. Відтак, зростає усвідомлення важливості проблем регулювання суспільних інформаційних відносин, зокрема узгодження принципово різних підходів до концептуального вирішення питання виокремлення та формулювання поняття “інформаційний суверенітет”, уточнення його характеристик для виявлення відповіді на питання про методи й засоби його збереження та вдосконалення. Для України така правова категорія є особливо важливою, оскільки гібридна війна, розв'язана Росією ставить питання існування суверенної Української держави в безпосередню залежність від забезпечення інформаційного суверенітету держави.

Результати аналізу наукових публікацій. У науковій літературі питання забезпечення інформаційного суверенітету відображені у наукових працях О. Баранова [1], О. Довганя [2], М. Ожевана, Д. Дубова [3], В. Супруна [4], а також наукових працях В. Пилипчука, В. Брижка [5; 6], І. Дороніна [7], що стосуються окремих напрямів регулювання суспільних відносин в інформаційній сфері. Проте актуальні умови розвитку інформаційних стратегій породжують нові вимоги до забезпечення інформаційного суверенітету та загострюють необхідність напрацювання комплексного підходу до дослідження його правової регламентації.

Метою статті є визначення правових підходів до поняття “інформаційний суверенітет держави” та його забезпечення в сучасних умовах.

Виклад основного матеріалу. Суверенітет – верховенство народу, нації, держави у внутрішній та зовнішній політиці, що забезпечує незалежність та самостійність розвитку суспільства. Є три основні типи суверенітету: державний, народний та національний. Ці типи суверенітету не тотожні, бо кожен має власний самостійний суб’єкт: державний – державу, народний – народ, національний – націю. Усі ці суверенітети органічно пов’язані, тісно переплетені. В мононаціональній державі національний, народний і державний суверенітети збігаються, знімаючи основні суперечності й проблеми. У багатонаціональній державі діалектика взаємовідносин досить складна. Національний і державний суверенітети є різними формами проявів народного суверенітету: перший відбиває його етнічну організацію, другий – державну. Таке розуміння взаємовідносин національного, народного і державного суверенітетів є найбільш поширеним і набуло юридичного закріплення в міжнародному праві [8].

Державний суверенітет є однією із найбільш дискусійних проблем юридичної науки. Особливої гостроти ці дискусії набули в другій половині ХХ ст., що пов’язано з одного боку з процесами внутрішньодержавної регіоналізації, а з другого – створенням наддержавних об’єднань у рамках процесу інтеграції [9]. Державний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності на своїй території (внутрішній суверенітет) та рівноправності і незалежності у відносинах з іншими державами (зовнішній суверенітет).

Загалом, тлумачення поняття “суверенітет держави” в енциклопедичних джерелах, як правило, пов’язані з визначенням меж суверенітету державними кордонами. Однак, сучасні процеси інформатизації, потужні інформаційні обміни в рамках глобального інформаційного простору значною мірою розмивають територіально-географічні особливості суверенітету як такого, а під впливом тенденцій розвитку інформаційного суспільства акценти державного суверенітету дещо змінюються і на перший план виходить його інформаційна складова, інформаційний суверенітет держави

Поняття “інформаційний суверенітет” є відносно відокремленим видом державного суверенітету, оскільки ознаки державного та інформаційного суверенітетів не завжди збігаються. Відтак, інформаційний суверенітет держави, хоча і може розглядатися як видовий відносно суверенітету держави, відрізняється від останнього юрисдикційними межами, колом уповноважених суб’єктів та ступенем участі недержавних структур у забезпеченні, власними моделями і комбінаціями методів правового регулювання, рівнем міжнародної співпраці тощо.

Науковцями неодноразово наголошувалось, що перед практиками у сфері забезпечення національної безпеки постає питання формування у свідомості населення розуміння феномену інформаційного суверенітету та автономії національної свідомості [10].

У національному законодавстві єдине визначення інформаційного суверенітету міститься в Законі України “Про Національну програму інформатизації” від 1998 р. як “здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави” [11].

Національні інформаційні ресурси є першоосновою інформаційного суверенітету, за їх допомогою держава контролює та регулює інформаційні потоки. Поряд із цим, поняття “інформаційні ресурси” також потребує належного наукового та юридичного обґрунтування. Це головний ресурс людської діяльності. В сучасних наукових дослідженнях цей ресурс розглядається в двох вимірах. У широкому значенні інформаційний ресурс – це важливий засіб, джерело соціальних перетворень. У вузькому значенні – це продукт виробництва та обміну, об’єкт протиборства і суперництва, сировина для цілеспрямованої (доцільної) соціально-економічної діяльності людини, під час якої створюється інформаційний (інтелектуальний) продукт і задовольняються потреби й інтереси людини. Отже, зміст інформаційного ресурсу – це система чи сукупність засобів задоволення інформаційних потреб людини. Як будь-яка система, інформаційні ресурси та інформаційна інфраструктура постійно змінюються, відповідно змінюється і їхній зміст [2].

Паралельно з поняттям “інформаційний суверенітет” у науковій літературі зустрічається ще поняття “цифровий суверенітет”. У випадку інформаційного суверенітету йдеться про ширше коло понять, яке включає не лише здатність впливати на інформаційно-комунікаційні технології загалом, але і на контент, причому далеко не завжди вплив слід розуміти як контроль, бо йдеться водночас про протидію інформаційно-психологічним операціям чи здійснення власних операцій. У розуміння ж цифрового суверенітету вкладається смисл пріоритетних завдань щодо забезпечення ІКТ-незалежності держави, тоді як до контентної частини терміна звертаються лише епізодично, на рівні збирання певних конкретних даних. Дедалі частіше у західних наукових працях з’являється поняття “кібермогутність”, під яким мають на увазі або “здатність до використання кіберпростору для створення переваг та впливу в усіх інших операційних просторах через інструменти могутності” або “можливість країни здійснювати заходи та впливати на кіберпростір” [3]. Дотичним до цього є поняття “суверенізація Інтернету”.

Загалом в міжнародному праві кібервійни зазначено наступне ставлення до суверенітету в кіберпросторі. Перше правило Талліннського статуту (Tallinn Manual) щодо міжнародного права, яке може бути застосовано до кібервійни, визначає загальні підходи до суверенітету в кіберпросторі. Зокрема визначено, що держава може здійснювати контроль над кібер-інфраструктурою і діяльністю в межах своєї суверенної території. Тобто суверенітет держави щодо об’єктів, на які він розповсюджується, є похідним від суверенітету держави щодо певної території. Зазначене стосується і об’єктів кібер-інфраструктури. За таких умов держава дійсно має суверенні права щодо встановлення обмежень, у тому числі і у питанні доступу до мережі Інтернет на власній території. Питання можливого порушення суверенітету внаслідок проведення операцій в кіберпросторі (кібервійна), а також пріоритету прав людини у цьому контексті, що визначені міжнародно-правовими актами, є досить складними і комплексними, їх однозначне трактування є справою майбутнього, про що свідчить характер наукової дискусії в цьому напрямку.

Таким чином, суверенне право держави мати контроль над об’єктами кібер-інфраструктури на своїй території під сумнів не ставиться. Але суверенітет не означає

наявності права власності або необхідності розповсюдження на ці об'єкти прямого державного управління. Отже, зазначені законодавчі новели ніякої суверенізації не встановлюють. Мова йде лише про посилення державного регулювання певної сфери [7]. В даному випадку мережі Інтернет.

На нашу думку, інформаційний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі. Цифровий суверенітет є різновидом інформаційного суверенітету.

Під єдиним інформаційним простором країни розуміють сукупність інформаційних ресурсів та інформаційної інфраструктури, що уможлиблює на основі єдиних принципів і за загальними правилами забезпечувати безпечну інформаційну взаємодію держави, організацій і громадян за їх рівного доступу до відкритих інформаційних ресурсів, а також максимально повне задоволення їх інформаційних потреб на усій території держави за збереження балансу інтересів на входження у світовий інформаційний простір та забезпечення національного інформаційного суверенітету [12].

Загалом, у нормотворчій практиці більш усталеним є використання поняття “інформаційний простір”, а стосовно інформаційно-комп'ютерних технологій та програмних продуктів – “кіберпростір”. Термін “віртуальний простір” переважно розглядається як синонімічний. Однак, Баранов О.А. вважає, що введення подібних абстрактних понять (“віртуальний простір”, “Інтернет-середовище”, “кібернетичний простір”), які відображають умовне уявлення людини щодо певних процесів, що супроводжують її діяльність, може бути виправдане лише з точки зору методологічного “виділення” деякої сукупності явищ при проведенні досліджень в певних наукових сферах, за винятком юридичної, яка розглядає суспільні відносини, що мають місце виключно в реальному, об'єктивному світі [1, с. 215].

Варто зауважити, що про будь-який суверенітет доцільно говорити лише за умови наявних можливостей його підтримання на належному рівні. Забезпечення інформаційного суверенітету України повинно включати: створення комплексної нормативно-правової регламентації визначення поняття “інформаційний суверенітет держави”, напрямів його забезпечення (законодавче визначення та забезпечення стратегічних напрямів розвитку і захисту національного інформаційного простору, визначення норм, засад і меж діяльності зарубіжних та міжнародних суб'єктів у національному інформаційному просторі України); повноважень відповідних органів та їх координації і взаємодії; участь у створенні та розвитку норм міжнародного права з огляду на інтеграцію у глобальний інформаційний простір.

Відтак, функція держави як основного суб'єкта забезпечення інформаційного суверенітету зводиться не лише до контролю інформаційних потоків, але й передбачає здійснення державою інформаційного впливу на своїх громадян з метою забезпечення національних інтересів держави в інформаційній сфері. Це повинно мати вираз у комплексній інформаційній політиці держави, яка б визначалась пріоритетністю національних інтересів, системою небезпек та здійснювалась шляхом прийняття та реалізації відповідних законів, доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

Разом з тим, Україна, як держава демократичних принципів, повинна в основу своєї інформаційної політики покласти принципи пріоритетності захисту індивідуальних, аніж державних інтересів. Стаття 34 Конституції України гарантує кожному право на свободу думки і слова, на вільне вираження своїх поглядів і

переконань; право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб і на свій вибір [13]. Реалізація цих прав може бути обмежена законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Ця норма ґрунтується на положеннях актів міжнародного законодавства, а саме: Загальної декларації прав людини (ст. 19), Конвенції про захист прав людини і основоположних свобод (ст. 10), Міжнародного пакту про громадянські і політичні права (ст.ст. 18, 19), Рекомендації Ради Європи № R(81)19 про доступ до інформації, що перебуває у володінні державних органів, Рекомендації Ради Європи № R (2002) про доступ до офіційних документів тощо.

Окрім цього, для того, щоб інформація правомірно обмежувалась у доступі, вона, згідно із запропонованим міжнародною неурядовою організацією Article 19 трискладовим тестом, повинна відповідати трьом вимогам, а саме: повинна мати відношення до легітимної мети визначеної законом; розголошення такої інформації повинно загрожувати спричиненням суттєвої шкоди визначеній законом меті; шкода, яка може бути заподіяною вказаній меті повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації [14].

В даному випадку необхідно дотримуватися двох принципів. Перший – принцип максимального оприлюднення: вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків. Другий принцип характеризує вимоги щодо обмежень: а) винятки повинні бути зрозумілими, б) описуватися вузько, в) підлягати контролю на предмет наявності “шкоди” і впливу на “суспільні інтереси”. А саме: рішення державного органу обмежити доступ до інформації є виправданим, якщо, по-перше, інформація має відношення до легітимної мети, передбаченої законом; по-друге, її оприлюднення має дійсно загрожувати спричиненням суттєвої шкоди легітимній меті; по-третє, шкода, яка може бути заподіяна вказаній меті, повинна бути вагомішою, ніж суспільний інтерес в отриманні інформації [15].

Багатьма науковцями виділяються наступні проблеми у зазначеній сфері: невпорядкованість термінології інформаційного законодавства; неправомірне застосування грифів обмеження доступу до інформації; проблема забезпечення пасивного доступу громадян до інформації; хаотичний розвиток інформаційного законодавства, що полягає в неузгодженості правових норм різних законодавчих актів; відсутність реальних механізмів забезпечення відповідальності за порушення інформаційного законодавства [16]. Відтак, висловлюються застереження, що орієнтація на інформаційну безпеку та інформаційний суверенітет може призвести до неправомірного обмеження права на інформацію.

Приймаючи нову редакцію Закону України “Про інформацію”, що набула чинності 9 травня 2011 р., законодавцем було враховано висновки експертів Ради Європи та вилучено поняття “інформаційний суверенітет”, що, на їх думку, “не належить до принципів, вжитих хоча б в одному договорі про захист прав людини” [17]. Проте, зважаючи на те, що сучасне розуміння демократичного, правового суспільства виходить з поваги і потреби захисту прав, свобод та безпеки людини на основі принципів законності та верховенства права, необхідно досягти балансу між правом на інформацію та вимогами щодо забезпечення інформаційної безпеки держави. Концепція свободи інформації, що була вперше запропонована на міжамериканській конференції 1945 р. у

Мехіко, передбачає свободу шукати, отримувати та поширювати інформацію будь-якими засобами й незалежно від державних кордонів. У 1946 р. свобода інформації як фундаментальне право людини було проголошено на першій сесії Генеральної асамблеї ООН у Резолюції 59 (I) “Скликання міжнародної конференції з питань свободи інформації”. Згодом ця концепція знайшла своє втілення в Загальній декларації з прав людини, Міжнародному пакті про громадянські та політичні права та інших міжнародних документах, що стосуються прав і свобод людини і громадянина.

В зарубіжному науковому дискурсі зазначені свободи частково реалізуються в понятті “інформаційний суверенітет особи”, а дефініція “інформаційний суверенітет” розкладається на складові інформація, приватність, суверенітет [18]. Хоча ми приєднуємось до тих науковців, які переконані, що таке розширення змісту поняття “суверенітет”, розповсюдження його на доволі широке коло суб’єктів фактично призводить до його девальвації. Юридична наука має інші загальновизнані терміни для визначення вказаних вище феноменів. Наприклад, замість суверенітету особи, слід говорити про її права та свободи, замість суверенності адміністративно-територіальних одиниць, мова повинна йти про місцеве самоврядування тощо. Категорія ж “суверенітет” має пов’язуватись виключно з державою, народом, нацією [19].

У розрізі забезпечення цифрового суверенітету держави необхідно враховувати права особи на приватність комунікацій – усе, що пов’язано з техніко-технологічними засобами і способами забезпечення телефонних розмов, електронних повідомлень, особистого поштового листування та інших видів інформаційно-комунікаційних зв’язків. При цьому, в умовах програмно-технологічного розвитку Інтернету приватність комунікацій все більше пов’язується з інформаційною приватністю, тобто з тим, що передбачає захист персональних даних людини, а також інформаційної безпеки людини, суспільства і держави. Ця тенденція безпосередньо стосується нових поглядів у застосуванні Інтернету, які отримали назву “Інтернет речей” та “Хмарні технології”. Технології типу “Інтернет речей” характеризують те, що кількість матеріальних об’єктів, підключених у світі до Інтернету, стала збільшуватися по відношенню до кількості людей, які взагалі користуються глобальними комунікаційними мережами. А “Хмарні технології” визначають перехід від використання окремих програмно-апаратних засобів, що належать окремим суб’єктам (компаніям), на модель створення та використання “відкритого об’єднання хмарних обчислень”, тобто “Хмарних технологій”, “Хмарних сервісів” [20, с. 207-217].

Висновки.

Актуалізація питань інформаційного суверенітету та підходів до його забезпечення обумовлена проникненням інформаційних технологій у всі сфери життя, здобуттям інформацією статусу найціннішого ресурсу. Загалом тема інформаційного суверенітету є важливою сьогодні для всіх держав без виключення.

На нашу думку, інформаційний суверенітет – це властивість державної влади, що полягає у її верховенстві, самостійності, повноті і неподільності в інформаційному просторі України та рівноправності і незалежності у відносинах з іншими державами у глобальному інформаційному просторі.

Разом з тим, сьогодні виникають нові поняття у сфері інформаційного суверенітету: цифровий суверенітет, інформаційний суверенітет особи, глобальний інформаційний простір, віртуальний простір тощо, які потребують наукового осмислення щодо включення в національне законодавство.

Проведений аналіз свідчить, що забезпечення інформаційного суверенітету України повинно включати: створення комплексної нормативно-правової регламентації

визначення поняття “інформаційний суверенітет держави”, напрямів його забезпечення, повноважень відповідних органів та їх координації і взаємодії; участь у створенні та розвитку норм міжнародного права з огляду на інтеграцію у глобальний інформаційний простір. Це повинно мати вираз у комплексній інформаційній політиці держави, яка б визначалась пріоритетністю національних інтересів, системою загроз та здійснювалась шляхом прийняття та реалізації відповідних законів, доктрин, стратегій, концепцій і програм в інформаційній сфері відповідно до чинного законодавства.

Забезпечення інформаційного суверенітету держави вимагає дотримання балансу між правом на інформацію та вимогами щодо обмежень в цілях забезпечення національної безпеки держави, між правом особи на приватність у інформаційній сфері, зокрема у комунікаціях, та забезпеченням цифрового суверенітету держави.

Використана література

1. Баранов О.А. Віртуальність і правове регулювання. *Публічне право*. 2017. № 1. С. 210-218.
2. Довгань О.Д. Національний інформаційний суверенітет – об’єкт інформаційної безпеки. *Інформація і право*. № 3(12)/2014. С. 102-112.
3. Ожеван М.А., Дубов Д.В. Номо ех Machina. Філософські, культурологічні та політичні передумови формування конвергентного суспільства: монографія. Київ: НІСД, 2017. 272 с.
4. Супрун В.М. Теоретико-правові основи інформаційного суверенітету: автореф. автореф. дис. ...канд. юрид. наук: 12.00.01 – Теорія та історія держави і права, історія політичних і правових учень. Харків. 2010. 21 с.
5. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. № 4(19)/2016. С. 60-70.
6. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с.
7. Доронін І.М. Правові проблеми суверенізації Інтернету. *Інформація і право*. № 2(29)/2019. С. 74-81.
8. Римаренко Ю.І. Суверенітет. – (Міжнародна поліцейська енциклопедія: у 10 т. / відп. ред. Ю.І. Римаренко, Я.Ю. Кондратьєв, В.Я. Тацій, Ю.С. Шемшученко). Київ: Концерн “Видавничий Дім “Ін Юре”, 2003. С. 990-991.
9. Байдін Ю.В. Державний суверенітет і його межі в умовах європейської інтеграції (питання теорії): автореф. дис. ...канд. юрид. наук.: 12.00.01 – Теорія та історія держави і права, історія політичних і правових учень. Харків. 2012, 20 с.
10. Савінова Н.А. Стратегії соціальних комунікацій як спосіб зниження соціальної напруги на макро-, мезо- та макрорівнях: зб. матер. наук.-практ. конф. *Актуальні проблеми управління інформаційною безпекою держави* (у 2-х ч. Ч. 1), м. Київ, 18 березня 2016 року. Київ: Нац. акад. СБУ, 2016. С. 148-152.
11. Про Національну програму інформатизації: Закон України від 04.02.98 р. *Відомості Верховної Ради України*. 1998. № 27-28. Ст.181.
12. Макаренко Є.А. Європейська інформаційна політика: монографія. Київ: Наша культура і наука, 2000. 368 с.
13. Конституція України: Закон України від 28.06.96 р. *Відомості Верховної Ради України*. 1996. № 30. Ст.141.
14. Принципи законодавства про свободу інформації. Стаття 19. Лондон, червень 1999. URL: <http://www.khpg.org/index.php?id=968017351> (дата звернення 01.03.2020).
15. Захаров Є. Свобода доступу до урядової інформації. Свобода висловлювань і приватність. – (Харківська правозахисна група). 2001. № 1. С. 14-18.
16. Березовська І. Актуальні питання доступу громадян до публічної інформації та проблеми застосування Закону України “Про доступ до публічної інформації”. URL: http://www.ena.lp.edu.ua:8080/bitstream/ntb/37396/1/5_26-31.pdf (дата звернення 15.09.2019).

17. Висновок експертів Ради Європи щодо проекту закону про інформацію. URL : <http://www.helsinki.org.ua /index.php?id=1173882959> (дата звернення 22.02.2020).

18. Polcak, R., & Svantesson, D. J. B. Information Sovereignty: Data Privacy, Sovereign Powers and the Rule of Law. Cheltenham: Edward Elgar Publishing, 2017. 217 с.

19. Гапотій В.Д. Суверенітет особи: суперечливість теоретико-правових підходів. *Вісник Запорізького юридичного інституту*. 2009. № 3. С. 3-10.

20. Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДПП НАПрН України). Київ: ТОВ “Видавничий дім “АртЕк”, 2019. 288 с.

~~~~~ \* \* \* ~~~~~

УДК 343.9.024:004.056

**ГУЦАЛЮК М.В.**, кандидат юридичних наук, доцент, головний науковий співробітник Міжвідомчого центру з проблем боротьби з організованою злочинністю при РНБО України.

## ЗАГРОЗЛИВІ ТЕНДЕНЦІЇ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

**Анотація.** У статті досліджуються сучасні тенденції кіберзлочинності, у тому числі її організовані форми, надаються пропозиції щодо посилення протидії цьому явищу.

**Ключові слова:** кіберзлочинність, кібератака, Даркнет, електронні докази.

**Summary.** The article deals with current trends in cyber crime, including its organized forms, and proposes to strengthen the counteraction to this phenomenon.

**Keywords:** cyber crime, cyber attack, Darknet, electronic evidence.

**Аннотация:** В статье исследуются современные тенденции киберпреступности, в том числе ее организованные формы, представлены предложения по усилению противодействия этому явлению.

**Ключевые слова:** киберпреступность, кибератака, Даркнет, электронные доказательства.

**Постановка проблеми.** Сучасний глобальний світ характеризується широким використанням переваг кіберпростору для отримання інформації, віддаленої роботи, взаємодії з державними органами, Інтернет-торгівлі тощо. Водночас інформаційні технології стали потужним інструментом для злочинців, який вони можуть використовувати для протиправної діяльності, у тому числі на транснаціональному рівні, для фінансового шахрайства, викрадення інформації, незаконного поширення наркотичних засобів тощо. Протиправна діяльність у кіберпросторі створює тіньову економіку, яка за доходами порівняна з економікою деяких держав.

Інтернет забезпечує злочинцям доступ до потенційних жертв у будь-якому куточку світу. Кіберзлочинці використовують властивість електронних даних миттєво передавати інформацію у кіберпросторі на значні відстані. Також Інтернет використовується для обміну знаннями та таємного спілкування, продажу викрадених даних, товарів та послуг, відмивання доходів, одержаних злочинним шляхом, а також обміну тактиками та інструментами кіберзлочинності.

Кіберзлочинність постійно та активно розвивається за складністю та організаційною спроможністю, а за багатьма аспектами вона сформована подібно до великого підприємства з ієрархічною структурою, в якій кожен має чітко визначену роль та відповідальність. Організатори таких структур контролюють проведення операцій, визначають стратегію та бізнес-модель, інспектують виконання плану. Основою злочинного бізнесу є технології, групи фахівців, які здатні розгорнути складні зловмисні програми, організувати приватні ботнети та створити фіктивні антивірусні програми, а також набори інструментів для несанкціонованого доступу до комп'ютерних систем. Для проведення масштабних кібероперацій спеціальні підрозділи розробляють програми набору персоналу, для пошуку виконавців з конкретними технологічними профілями під конкретну кібератаку.

У зв'язку із значним негативним впливом кіберзлочинності на цифрове суспільство це явище в останні роки досліджувалось як окремими науковцями, так і установами та організаціями через призму кримінології, криміналістики, психології, соціології, а також

інших наукових дисциплін. Подальше зростання кількості кіберзлочинів, збитків цифрової економіки від них та суттєве ускладнення кібератак спонукає проведення подальших досліджень щодо протидії кіберзлочинності та в особливості її організованим формам.

**Результати аналізу наукових публікацій.** У зв'язку із значним негативним впливом кіберзлочинності на цифрове суспільство це явище досліджувалось багатьма закордонними Maras Marie-Helen, Eoghan Casey, Thomas J. Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar та вітчизняними вченими Н. Ахтирська, П. Біленчук, В. Бутузов, В. Гавловський, О. Кравцова, А. Марущак, К. Тітуніна, В. Шеломенцев, В. Хахановський, О. Юрченко та інші.

В той же час сьогодні ще не достатньо досліджені особливості діяльності організованих злочинних угруповань (далі – ОЗУ) у кіберпросторі та методи і способи виявлення та розслідування їх діянь та боротьби з ними.

**Метою статті** є дослідження сучасного стану організованої кіберзлочинності та визначення основних тенденцій її розвитку.

**Виклад основного матеріалу.** Починаючи з 2000-х років у зв'язку з широким поширенням Інтернету по всьому світу проблема боротьби з кіберзлочинністю набула міжнародного характеру. Ще у 2001 р. Генеральна асамблея ООН резолюцією 55/63 від 22 січня 2001 року [1] на виконання Декларації тисячоліття Організації Об'єднаних Націй щодо забезпечення усіх благами нових інформаційно-телекомунікаційних технологій рекомендувала вжити низку наступних заходів:

- держави повинні забезпечити, щоб їх законодавство і практика не залишали можливості тим, хто зловживає інформаційними технологіями, ховатися де б то не було;
- співробітництво правоохоронних органів у розслідуванні випадків транскордонного злочинного використання інформаційних технологій і судове переслідування в зв'язку з цим має координуватися усіма відповідними державами;
- держави повинні обмінюватися інформацією про проблеми, з якими вони стикаються в боротьбі зі злочинним використанням інформаційних технологій;
- режими взаємної допомоги повинні забезпечувати своєчасне розслідування випадків злочинного використання інформаційних технологій і своєчасний збір доказів і обмін ними в подібних випадках;

У 2011 році в ООН була створена Міждержавна група експертів з вивчення кіберзлочинності, зусиллями якої у 2013 році було проведено “Всебічне дослідження проблеми кіберзлочинності”. У цьому документі проаналізовані такі аспекти як законодавство у даній сфері, діяльність правоохоронних органів, міжнародне співробітництво тощо. В ньому, зокрема, зазначається, що 80 відсотків кіберзлочинів вчиняється в організованій формі [2].

Робота міждержавної групи експертів продовжується і сьогодні. Так у доповіді за наслідками наради даної групи 27-29 березня 2019 року у Відні були розглянуті питання удосконалення законодавства, у тому числі міжнародного, проблеми діяльності правоохоронних органів, використання електронних доказів. Було зазначено, що, зважаючи на транснаціональний характер кіберзлочинності і той факт, що значна більшість глобальних кіберзлочинів вчиняються організованими групами, державам-членам слід більш широко застосовувати Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності для сприяння обміну інформацією та доказами в ході кримінальних розслідувань, що стосуються кіберзлочинності [3].

Термін “кіберзлочин” визначено Законом України “Про основні засади забезпечення кібербезпеки України”. Види кіберзлочинів визначені у Конвенції про кіберзлочинність 2001 року, яка була ратифікована Законом України від 07.09.05 р. № 2824-IV. Кіберзлочини можна поділити на власне кіберзлочини, метою вчинення яких є порушення конфіденційності, доступності або цілісності інформації в комп’ютерній системі (несанкціонований доступ до комп’ютерних систем, атаки на відмову в обслуговуванні, незаконне перехоплення комп’ютерних даних тощо), та кіберзалежні злочини, які вчиняються з використанням інформаційно-комунікаційних технологій, наприклад шахрайство. На сьогодні в чинному українському законодавстві поки що не визначено чіткого переліку статей Кримінального кодексу України, які слід відносити до кіберзлочинів.

На практиці злочинці можуть вчиняти декілька видів кіберзлочинів послідовно або навіть одночасно. Наприклад, у 2017 році кіберзлочинці вчинили несанкціонований доступ до системи відомого литовського пластичного хірурга та отримали конфіденційну інформацію про пацієнтів із різних куточків світу, про процедури, які вони проводили, 25000 фотографій оголених пацієнтів та медичні дані. Після цього кіберзлочинці погрожували кожному пацієнтові оприлюднити цю інформацію у разі, якщо не буде сплачено викуп. Вартість викупу змінювалася залежно від кількості та якості викраденої інформації про пацієнта [4].

Зазначимо, що більшість досліджень вказують на зростання як кількості кіберзлочинів, так і збитків від них. Наприклад, лише у Лондоні за період із квітня по вересень 2018 року було зареєстровано 13357 кіберзлочинів, від яких потерпіли втратили 34,6 мільйона фунтів стерлінгів. Кількість інцидентів продовжує зростати. За словами начальника поліції міста Лондона Карен Бакстер, “кіберзлочинність – це зростаюча тенденція, загальні збитки від якої щорічно збільшуються на 24 відсотки”. Уряд Великобританії серйозно сприймає цей ризик, визначаючи кіберзлочинність як загрозу національній безпеці першого рівня та вкладаючи майже 2 мільярди фунтів у Національну стратегію кібербезпеки, розроблену для її протидії [5].

В Україні за останні п’ять років кількість інформаційних злочинів зросла щонайменше у 2,5 рази. Про це повідомляє прес-служба Opendatabot. Збільшення кількості всіх кіберзлочинів відбулося у 2017 році, що значною мірою пов’язано з вірусом Petya. Відтоді кількість інформаційних злочинів не зменшується [6].

Збитки від кіберзлочинів можуть коливатися від кількох доларів до кількох мільярдів доларів. Наприклад, вірус Petya спричинив збитків по всьому світі на 8 млрд доларів. Тільки вітчизняна Укрпошта зазнала збитків у 100 млн гривень [7]. Кількість викраденої або модифікованої інформації також може значно відрізнятися в різних випадках. Наприклад, У січні 2019 року на хмарному сервісі MEGA була виявлена база даних користувачів із майже 773-ма мільйонами адрес електронної пошти і 22-ма мільйонами унікальних паролів. Це був найбільший витік викрадених даних з усіх відомих обсягом 87 гігабайт [8].

Особливе занепокоєння викликає активний розвиток упродовж останніх років такого явища, як “кіберзлочин-послуга” – он-лайн-ринку для обміну викраденими даними, хакерськими інструментами й уразливостями інформаційних систем, а також іншими кримінальними послугами, такими як оренда бот-мереж і спам-серверів. Також на цьому “ринку” надають послуги, які полегшують вчинення злочинів та кіберзлочинів, такі як дані та документи, що посвідчують особу (наприклад, фінансові та медичні дані, паспорти тощо); зловмисне програмне забезпечення (тобто, виготовлене на замовлення або вже відоме зловмисне програмне забезпечення – наприклад, Zeus (“Зевс”)),

банківський троян, розроблений для прихованого захоплення банківських даних користувачів; кібератак відмови в обслуговуванні (DDoS) та ботнет-послуг; інструменти фішингу; хакерські підручники; а також інформацію про вразливості різноманітних інформаційних ресурсів та інструкції, як ними скористатися).

Вартість таких послуг досить помірنا. Наприклад, у Звіті Underground Hacker Marketplace зазначено, що дані кредитної картки можна придбати за 30 доларів США, набори інструментів для віддаленого доступу до комп'ютера всього за 5 доларів США та розподілені атаки типу "відмова в обслуговуванні" на певних сайтах всього за 5 доларів США на годину [9].

А у дослідженні "Cybercrime and the Underground Market [Updated 2019]" приведено наступні приклади продажу шкідливого програмного забезпечення [10]:

"Продам вихідний код Zeus 2.0.8.9. Приватний продаж вихідного коду. Ціна: 400–500 доларів США; можливі торги (можлива заміна)".

"Налаштування Zeus: 100 доларів США, підтримка ботнету: 200 доларів США на місяць, консультація: 30 доларів США".

Модель продажу "зловмисне програмне забезпечення як послуга" є дуже небезпечною, оскільки надає можливість для звичайних злочинців без особливих знань здійснити серйозні кібератаки на банківські системи. У деяких випадках, щоб захистити свою анонімність, виробники зловмисного програмного забезпечення розгортають продаж своїх виробів у Darknet.

Наприклад, розробник "Butterfly Bot" рекламував це шкідливе програмне забезпечення в Інтернеті як таке, що здатне взяти під контроль комп'ютери Windows та Linux. Він також продавав плагіни (plug-in – додаток, що динамічно підключається до основної програми), які модифікували функції зловмисного програмного забезпечення. Різноманітні кримінальні мережі поширили цей Butterfly Bot, унаслідок чого цією шкідливою програмою були заражені **12,7 мільйона** комп'ютерів у всьому світі. Улітку 2019 року розробник "Butterfly Bot" був заарештований німецькою поліцією [11].

У січні 2019 року міжнародна спільна слідча група, до складу якої входили співробітники Генеральної прокуратури України, Національної поліції України, а також правоохоронців з Бельгії, за сприяння Європолу та ФБР США провели обшуки у дев'яти локаціях в Україні.

Четверо українців віком від 27 до 37 років створили та підтримували діяльність відомого у Darknet ресурсу "xDedic", що давав змогу користувачам продавати й купувати доступ до зламаних серверів, викрадення банківських коштів, конфіденційної інформації, блокування інформації вірусами-вимагачами тощо

Щорічний дохід кожного із організаторів групи налічував більш як 1.2 млн доларів. Отримані кошти фігуранти зберігали в електронних гаманцях криптовалютних електронних систем та періодично виводили їх у готівку через неофіційні обмінні пункти. Одночасно із обшуками були заблоковані доменні імена, необхідні для функціонування xDedic [12].

Слід зазначити, що широкий спектр постачальників послуг в Інтернеті активно експлуатується терористичними групами. Вони використовують найновіші технології для он-лайн спілкування. Тому при вдалому плануванні та підтримці прихильників терористів кібератаки, організовані терористами, можуть поширюватися швидше, ніж провайдери та правоохоронні органи зможуть на них відреагувати.

Багато ОЗУ використовують Інтернет-технології для зв'язку правопорушників щодо скоєння традиційних злочинів, після чого злочинна організація припиняє діяльність, щоб знову утворити нову. Крім того, ОЗУ можуть використовувати мережеві

технології для створення більш “стійких” організаційних форм, для захисту злочинців, що працюють під їх “дахом”, від інших злочинців у цій сфері, а також правоохоронних органів. Між цими двома крайнощами спектру існують також “гібридні” форми. Часто члени таких злочинних організацій знають один про одного лише через нікнейми (вигадані імена), що значно ускладнює розслідування діяльності таких груп.

Наприклад, злочинці використовують інформаційно-комунікаційні технології (далі – ІКТ) для удосконалення різних форм традиційної оф-лайн-організованої злочинності, таких як контрабанда мігрантів та торгівля людьми, наркотиками, вогнепальною зброєю та цигарками.

Наприклад, співробітниками БКОЗ СБ України спільно з поліцією Ізраїлю припинена діяльність найбільшої за останні десятиліття міжнародної мережі Інтернет-торгівлі наркотиками.

Правоохоронці встановили, що у 2017 році громадянин Ізраїля в одному із соціальних месенджерів створив Інтернет-канал для збуту оптових партій наркотичних засобів та психотропних речовин. За кілька років нелегальний бізнес розширився, і такі “торговельні майданчики” почали функціонувати в інших соціальних мережах. За даними ізраїльської поліції, географія злочинної діяльності наркоторгівців розповсюджувалася на країни Південної та Північної Америки, Європейського Союзу, Близького Сходу, Азії та Африки. У синдикат входило понад тринадцять тисяч осіб, у тому числі контрабандисти, дилери, адміністратори груп у соцмережах.

У березні 2019 року на підставі клопотання про міжнародну допомогу українські правоохоронці затримали главу наркокартеля в Києві, куди він прибув для налагодження “бізнес-зв’язків” із представниками місцевих кримінальних кіл. Одночасно в Ізраїлі було затримано 42 особи [13].

При вивченні організованої кіберзлочинності слід враховувати цільову групу потерпілих. Деякі злочинні групи навмисно атакують окремих користувачів, щоб вчинити шахрайство чи шантаж. Інші групи зорієнтовані на середній бізнес чи урядові організації і вчиняють шахрайство більш масштабного обсягу. Нарешті, як правило, спеціальні державні суб’єкти свідомо націлюють свою діяльність на інфраструктуру інших держав, щоб створити недовіру до них чи вчинити масштабні кіберзлочини. Кількість учасників таких угруповань може коливатися від кількох злочинців до кількох тисяч, які вчиняють скоординовані дії.

Наприклад, Shadowcrew – “міжнародна організація”, нараховувала близько 4000 членів та сприяла широкому спектру злочинних дій, включаючи, серед іншого, електронні крадіжки особистої ідентифікаційної інформації, шахрайство з кредитними картками, а також виробництво та продаж фальшивих ідентифікаційних документів [14].

Незаконні товари та послуги в мережі Інтернет та в закритій її частині Darknet в основному купуються за допомогою криптовалют. На ринку є чимало криптовалют (наприклад, Bitcoin, Litecoin, Dogecoin, Ethereum та Monero). Водночас більшість ринків Darknet в основному використовують Ethereum і Monero через те, що відслідкувати переказ таких платежів украй складно.

Зазначимо також, що обіг криптовалют в Україні законодавчо не визначений, що також ускладнює розслідування кіберзлочинів та вилучення коштів, здобутих злочинним шляхом. Сьогодні на розгляді Верховної Ради України знаходиться проєкт закону “Про внесення змін до Податкового кодексу України та деяких інших законів України щодо оподаткування операцій з криптоактивами” (реєстр. № 2461 від 15.11.19 р.), в якому будуть надані базові визначення криптовалют. Разом із тим, цей законопроект

стосується лише сфери оподаткування та не охоплює питань, пов'язаних із кримінальними провадженнями.

Варто зазначити, що відповідно до дослідження X-Force Threat Intelligence Index кожне окреме ОЗУ спеціалізується на конкретному шкідливому програмному забезпеченні і зосереджується на різних частинах земної кулі. Проте з 2018 року виявилася нова тенденція – різні ОЗУ почали співпрацювати між собою для організації широкомасштабних операцій у банківській сфері. Така тенденція співпраці між троянськими операторами пояснюється бажанням отримати більший прибуток, незважаючи на вдосконалення контролю безпеки в банківській сфері [15].

У листопаді 2019 року на Черкащині Служба безпеки України припинила діяльність міжнародного хакерського угруповання, учасники якого викрадали кошти з рахунків користувачів електронних платіжних систем Європи та США.

Оперативники спецслужби встановили, що організаторами оборудки є громадянин РФ, який проживає у Києві, та троє мешканців Черкащини. Кіберзлочинці через спеціальні закриті хакерські форуми купували дані платіжних рахунків іноземців. За привласнені кошти вони закуповували товари у популярних закордонних Інтернет-магазинах. Потім продукцію реалізовували в Україні через онлайн-сервіси. Діяли хакери з 2010 року, їх річний обіг становив 500-700 тисяч доларів США.

Наразі вирішується питання щодо здійснення зловмисникам повідомлення про підозру у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 361 та ч. 2 ст. 209 Кримінального кодексу України [16].

Європол створив Європейський центр кіберзлочинності (далі – ЕСЗ) у 2013 році, щоб посилити реагування правоохоронних органів на кіберзлочинність у ЄС і таким чином допомогти захистити європейських громадян, підприємств та уряди від злочинності в Інтернеті. З моменту свого створення ЕСЗ зробив вагомий внесок у боротьбу з кіберзлочинністю: він був залучений до десятків гучних операцій та сотень оперативних розгортань на місці, що призвели до сотні арештів, і проаналізував сотні тисяч файлів, переважна більшість з яких виявилася шкідливою.

Вагомий внесок у боротьбу з організованою кіберзлочинністю вносить Європол, який для посилення реагування правоохоронних органів на кіберзлочинність у ЄС у 2013 році створив Європейський центр кіберзлочинності (ЕСЗ), який брав участь у десятках гучних спеціальних операцій та проаналізував сотні тисяч файлів, що призвело до сотень арештів кіберзлочинців.

Починаючи з 2011 року Європол щорічно готує та оприлюднює звіт про оцінку загроз організованої кіберзлочинності – ІОСТА (Internet Facilitated Organised Crime Tread Assessment) [17]. Завдяки матеріалам ІОСТА визначаються реальні та потенційні загрози у кіберпросторі для країн-членів ЄС, можливі сценарії реагування на них. Європейський Союз та його інформаційно-комунікаційні мережі й інфраструктура залишаються найбільш уразливими об'єктами для кіберзлочинців.

У 2019 році експерти Європолу дійшли таких висновків.

#### ***Віруси-вимагачі (ransomware).***

На даний час віруси-вимагачі (ransomware) залишаються найбільшою загрозою. Хоча загальний обсяг кібератак знизився, проте зловмисники зосереджуються на меншій кількості цілей, проте з більшим економічним збитком.

Найбільш значимі кібератаки у 2019 році були здійснені проти органів місцевого самоврядування, зокрема в Сполучених Штатах. Ця тенденція розпочалася раніше, коли у 2018 році кібератака паралізувала місто Атланта протягом декількох тижнів. Після цього вже більше півтисячі міст і різноманітні державні служби США стали жертвою

вірусу-вимагача викупу, у зв'язку з чим губернатор Луїзіани навіть оголосила надзвичайну ситуацію у штаті.

Також на початку листопада 2019 року спрямовані атаки вірусу-вимагача вивели з ладу дві іспанські компанії в один день: велику фірму Everis, що належить NTT Data Group і працює у сфері IT-послуг та консалтингу, а також радіокомпанію Sociedad Española de Radiodifusión [18]. Багато компаній, у тому числі іспанський оператор аеропорту Aena, відмовилися від ряду послуг в якості запобіжного заходу.

24 жовтня 2019 року в ході цілеспрямованої кібератаки хакери зламали комп'ютерну мережу міста Йоганнесбург (ПАР). Вони за допомогою вірусу-вимагача заблокували дані міської адміністрації і обіцяли повернути їх тільки після виплати викупу. Група кіберзлочинців, відома під назвою Shadow Kill Hackers, вимагала виплати чотири біткойни (\$ 30 000) [19].

11 листопада 2019 року мексиканська державна нафтогазова корпорація Pemex повідомила про атаку вірусу-зидника на свої комп'ютери, в результаті якої вона змушена була припинити адміністративну роботу. Хакери вимагали викупу у 5 млн доларів США [20].

Зниження кількості кібератак можна пояснити низкою причин, серед яких:

- підвищення обізнаності щодо основ кібербезпеки серед користувачів;
- правозастосовні ініціативи для зменшення наслідків загроз (наприклад, NoMoreRansom);
- збільшення використання мобільних пристроїв серед користувачів (більша частина програм-вимагачів зорієнтована на Windows) тощо.

#### ***DDOS-атаки.***

Значною загрозою для інформаційних систем включно з критичною інфраструктурою залишаються DDos-атаки. Іноді вплив таких атак на он-лайн-банківські сервіси завдає більше збитків, ніж прямі атаки з метою пошкодження даних в комп'ютерних системах.

У Даркнеті ще залишаються поширеними нелегальні ринки збуту послуг з організації DDos-атак.

Під час проведення у квітні 2018 року спільної операції правоохоронних органів із десяти країн "Power Off" за підтримки Європолу було виявлено базу даних із 150000 зареєстрованих користувачів таких послуг та джерело 4 мільйонів кібератак.

У 2019 році правоохоронці долучилися до значно ширшого кола різноманітних розслідувань нападів на об'єкти критичної інфраструктури, включаючи енергетику, транспорт, водопостачання, галузь охорони здоров'я тощо.

У березні 2019 року норвезька компанія NorskHydroAS – постачальник відновлюваної енергії та один з найбільших виробників алюмінію у світі був скомпрометований програмою-вимагачем LockerGoga через цілеспрямовану кібератаку. Кібератака суттєво вплинула на бізнес, у результаті чого сталися перебої виробничих потужностей в Європі та США. Компанія зазнала збитків до 350 мільйонів норвезьких крон ( $\approx 35$  млн. Євро) [21].

За допомогою іншого вірусу-вимагача Locker GOGA були здійснені атаки на понад 1200 промислових об'єктів по всьому світу. Правоохоронні органи Франції у грудні 2019 року звернулися до українських силовиків із проханням допомогти в пошуку хакерів. Як встановили французькі правоохоронці, деякі поштові скриньки і IP-адреси низки електронних скриньок (через які відбувалося зараження) належать Україні.

Співробітники Департаменту кіберполіції Національної поліції України встановили чотирьох можливих учасників злочинного угруповання. Слідство триває [22].

У відповідь на великі транскордонні кібератаки необхідно використовувати механізми міжнародного співробітництва, включаючи можливості підтримки Інтерполу, Європолу, Євроюсту та юридичних інструментів, розроблених для транскордонної співпраці (такі як Міжнародні спільні слідчі групи (Joint Investigation Team – JITs) та Спільні робочі групи з питань кіберзлочинності (Joint Cybercrime Action Taskforce – J-CAT) з метою обміну ресурсами та координації дій.

Успішна робота таких груп неможлива без обробки електронних даних, які можуть знаходитись на серверах у різних частинах світу. Більшість таких комп'ютерів знаходяться у приватному секторі. Тому успішна боротьба зі злочинцями можлива лише при тісній співпраці правоохоронних органів та приватного сектору ІТ-індустрії. З іншого боку така співпраця дозволить приватному сектору проводити необхідну профілактику для кіберзахисту себе та своїх клієнтів.

3 лютого 2018 року Інтерпол бере участь у дослідницькому проєкті, який має на меті сприяти обміну електронними доказами в межах Європейського Союзу та активізувати міжнародну співпрацю щодо протидії злочинності. Його мета – створити інструмент для обміну електронними (цифровими) доказами через e-CODEX у рамках процедур взаємної правової допомоги [23].

Статті 16 та 17 Конвенції про кіберзлочинність від 2001 року передбачають прийняття країнами-підписантами Конвенції нормативних актів та процедур щодо термінового збереження комп'ютерних даних та часткового розкриття даних про рух інформації. На жаль, на сьогодні дані положення ще не імplementовані у Кримінальний процесуальний кодекс України. Також варто надати чіткі визначення електронних доказів та процедур щодо їх збирання.

У Комітеті Верховної Ради України з питань правоохоронної діяльності 10 грудня 2019 року створена робоча група щодо вдосконалення чинного законодавства з питань боротьби з кіберзлочинністю та використання електронних доказів, метою діяльності якої стала необхідність імplementації Будапештської Конвенції про кіберзлочинність у вітчизняне законодавство, пошук оптимальних шляхів удосконалення законодавчого забезпечення правоохоронної діяльності у цьому сегменті. Автором була внесена пропозиція щодо доповнення частини 2 статті 84 КПК України категорією “електронних доказів”, а саме “Процесуальними джерелами доказів є показання, речові докази, електронні докази, документи, висновки експертів”.

Відповідно до статистичної звітності Національної поліції України за 2019 рік Департаментом кіберполіції НП України виявлено 4 організовані групи, якими вчинено 84 кіберзлочини. За 2018 рік було виявлено 10 організованих груп, якими вчинено 119 кіберзлочинів. Очевидно, протиправною діяльністю сьогодні займаються ще не виявлені групи, що пояснюється високою латентністю кіберзлочинів. Наприклад за словами начальника підрозділу Центру розгляду скарг на кіберзлочини ФБР, загальна кількість кіберзлочинів, що повідомляються, становить лише 10 – 12 % від фактичної кількості [24].

Існує також кілька технічних причин, які ускладнюють боротьбу з кіберзлочинністю, у тому числі її організованими формами.

Перша причина – складність виявлення IP-адрес злочинців. Проблема полягає в тому, що є багато способів приховати IP-адресу або навіть підробити дані так, наче підключення здійснюється з іншої IP-адреси. Більш того, злочинці можуть використовувати різні інструменти, щоб уникнути виявлення їх правоохоронними органами, та приховати свої сайти у Darknet.

Інша технічна проблема пов'язана з уразливістю програмного забезпечення. Це дозволяє зловмисникам, наприклад, здійснювати несанкціонований доступ до

інформаційних систем. Іноді зловмисники знаходять уразливість раніше компанії, що виробляє програмне забезпечення (так звана уразливість “нульового дня”). Крім того, останнім часом хакери починають активно використовувати складні алгоритми “віруса-мутанта”, який складно виявити внаслідок постійної зміни сигнатури вірусу.

Уразливості призводять до втрати даних і є відносно поширеними навіть для великих організацій, оскільки завдання створення, налаштування і захисту цифрових систем належним чином є складною проблемою.

Дії, які вживаються для протидії кіберорганізований злочинності, зосереджуються на правоохоронних заходах, технічних рішеннях та освітніх кампаніях. Правоохоронні органи повинні здійснювати моніторинг веб-сайтів (як видимих, так і у Darknet), які сприяють кіберорганізований злочинності, виявлення цих сайтів та притягнення до відповідальності осіб, які організують злочинну діяльність. Як приклад успішних можна навести спільні операції правоохоронних органів США та Нідерландів щодо сайтів у Darknet AlphaBay та Hansa, на яких здійснювалися продажі різноманітних протизаконних товарів, таких як наркотики, банківські картки, зброя тощо. Розслідування під керівництвом США було спрямоване на AlphaBay. Коли доступ до AlphaBay був закритий, користувачі (продавці та покупці) платформ перейшли на інший сайт – Hansa, що знаходився під контролем нідерландської поліції, яка проводила таємну операцію з виявлення та припинення незаконної діяльності. Ця міграція дозволила голландським правоохоронцям ідентифікувати та притягнути злочинців до відповідальності. Розслідування AlphaBay та Hansa демонструють важливість міжнародного співробітництва.

Також для боротьби з кіберорганізованою злочинністю впроваджуються різноманітні технологічні рішення. Програмне забезпечення використовується для виявлення повідомлень у рекламі, які вказують на торгівлю людьми. Сьогодні широко застосовується технологія розпізнавання облич для ідентифікації жертв торгівлі людьми та сексуальної експлуатації дітей. Програмне забезпечення для розпізнавання зображень також може використовуватися для ідентифікації об'єктів дикої природи та незаконних товарів, таких як наркотики чи вогнепальна зброя. Це програмне забезпечення може прискорити ідентифікацію незаконних товарів в Інтернеті та вказати незаконний вміст для огляду модераторами веб-платформ.

Український стартап Traces AI розробив систему розпізнавання людей навіть не на основі облич, а завдяки аналізу 2000 інших параметрів, включаючи колір шкіри, тип і деталі одягу, зачіску, форму тіла та таке інше. Впровадження такої системи повинно бути досить ефективним, адже жертви торгівлі людьми зазвичай ховають своє обличчя [25].

Оскільки чисельність кіберзлочинів продовжує постійно зростати, необхідно посилювати спроможність кіберполіції. Водночас збільшення числа підрозділів кіберполіції потребує значного збільшення кількості необхідного кваліфікованого персоналу. Його підготовка здійснюється через масштабні навчальні програми. Наприклад, у 2018 році поліція Великобританії співпрацювала з Мережевою академією Cisco щодо навчання у сфері кібербезпеки для 120000 офіцерів. Також регулярно проводяться тренування поліцейських щодо спеціальних навичок з кібербезпеки, які охопили понад 80 відсотків особового складу по всій країні. Також були проведені спеціальні курси для слідчих, які присвячені поглибленому вивченню фізичних та логічних мереж, що охоплюють бездротові мережі, операційні системи Linux, логи та методи збору даних.

Проводяться і інші курси, які охоплюють принципи управління інформаційною безпекою, методи використання Інтернет-ресурсів для отримання інформації про підозрюваного тощо. Кримінальним слідчим необхідний розширений доступ до навчання методикам розслідування в Інтернеті, використанню та вилученню криптовалют, таких як біткойн, та вилученню доказів, отриманих у чатах та інтернет-комунікаціях [1].

### **Висновки.**

Організована кіберзлочинність постійно трансформується, у зв'язку з чим з'являються нові загрози та виклики, що потребує вжиття різноманітних заходів, у тому числі організаційного, правового та технічного характеру з метою адекватного превентивного захисту як користувачів кіберпростору, так і об'єктів критичної інфраструктури, банківської системи тощо.

Для посилення боротьби з кіберзлочинністю, у тому числі з її організованими формами пропонується:

1. Враховуючи, що організована кіберзлочинність носить транскордонний характер, необхідно посилити міжнародну співпрацю правоохоронних органів шляхом участі у спільних слідчих групах, та обміну інформацією, у тому числі оперативною, каналами Європолу та Інтерполу.

2. Провести імплементацію положень статей 16 та 17 Конвенції про кіберзлочинність щодо термінового збереження комп'ютерних даних та часткового розкриття даних про рух інформації.

3. Внести поняття “електронні докази” в Кримінальний процесуальний кодекс України, а також положення щодо особливостей їх отримання, зберігання та подання до суду.

4. Для поглибленого вивчення тенденцій організованої кіберзлочинності в Україні доцільно провести дослідження на основі методології звіту Європолу про оцінку загроз організованої кіберзлочинності – ЮСТА.

5. Постійно проводити навчання та перепідготовку слідчих Національної поліції України методикам розслідування кіберзлочинів, у тому числі на основі аналізу інформації з Інтернет.

### **Використана література**

1. Борьба с преступным использованием информационных технологий: Резолюция ООН от 22 января 2001 г. № 55/63. URL: <https://www.undocs.org/ru/A/RES/55/63> (дата звернення 14.01.2020).

2. Всестороннее исследование проблемы киберпреступности URL: [https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime\\_Study\\_Russian.pdf](https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf). С. 31 (дата звернення 14.01.2020).

3. Доклад о работе совещания Группы экспертов для проведения всестороннего исследования проблемы киберпреступности, проведенного в Вене 27–29 марта 2019 года. С. 4. URL: [https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC\\_CCPCJ\\_EG.4\\_2019\\_2\\_R.pdf](https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-March-2019/Report/UNODC_CCPCJ_EG.4_2019_2_R.pdf) (дата звернення 14.01.2020).

4. Hackers publish private photos from cosmetic surgery clinic. *The Guardian*, 31 May 2017. URL: <https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments>

5. Why police need the skills to counter cybercrime. URL: <https://www.raconteur.net/technology/police-skills-cybercrime> (дата звернення 14.01.2020).

6. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. URL: <https://www.mind.ua/news/20203511-kilkist-kiberzlochiviv-v-ukrayini-zroslo-vdvichi-za-ostanni-p-yat-rokiv-opendatabot> (дата звернення 14.01.2020).

7. “Укрпошта” зазнала 100-мільйонних збитків через вірус Petya. URL: <https://www.epravda.com.ua/news/2018/04/24/636312> (дата звернення 14.01.2020).
8. The 773 Million Record “Collection #1” Data Breach. URL: <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach> (дата звернення 14.01.2020).
9. Underground Hacker Marketplace Report. URL: <https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report> (дата звернення 14.01.2020).
10. Cybercrime and the Underground Market [Updated 2019]. URL: <https://www.resources.infosecinstitute.com/cybercrime-and-the-underground-market/#gref> (дата звернення 14.01.2020).
11. Mariposa Botnet Author, Darkcode Crime Forum Admin Arrested in Germany. URL: <https://www.krebsonsecurity.com/tag/butterfly-bot> (дата звернення 14.01.2020).
12. Найвідомішим у Darknet ресурсом заправляли українці – Кіберполіція. URL: <https://www.pravda.com.ua/news/2019/01/28/7205116> (дата звернення 14.01.2020).
13. У Києві затримали керівника одного з наймасштабніших наркосиндикатів у світі. URL: <https://www.unian.ua/incidents/10476900-u-kiyevi-zatrimali-kerivnika-odnogo-z-naymasshtabnishih-narkosindikativ-u-sviti-foto.html> (дата звернення 14.01.2020).
14. История разгрома ShadowCrew. URL: <https://www.kv.by/archive/index2005302201.htm> (дата звернення 14.01.2020).
15. X-Force Threat Intelligence Index 2019. URL: <https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf> (дата звернення 14.01.2020).
16. СБУ викрила хакерське угруповання на знятті коштів клієнтів електронних платіжних систем Європи та США. URL: <https://www.ssu.gov.ua/ua/news/1/category/2/view/6782#.xr1LH33i.dpbs> (дата звернення 14.01.2020).
17. Internet Organised Crime Threat Assessment (IOCTA). URL: <https://www.europol.europa.eu/iocta-report> (дата звернення 14.01.2020).
18. Ransomware attacks in Spain leave radio station in “hysteria”. URL: <https://www.nakedsecurity.sophos.com/2019/11/06/spanish-ransomware-hits-two-companies> (дата звернення 14.01.2020).
19. Shadow Kill Hackers cripple City of Jozi; demand Bitcoin ransom. URL: <https://www.biznews.com/briefs/2019/10/25/hackers-cripple-city-jozi-bitcoin-ransom> (дата звернення 14.01.2020).
20. A Hacker Wants About \$5 Million in Ransom From Pemex By End of November. URL: <https://www.bloomberg.com/news/articles/2019-11-13/a-hacker-wants-about-5-million-from-pemex-by-end-of-november> (дата звернення 14.01.2020).
21. In its ransomware response, Norsk Hydro is an example for us all. URL: <https://www.grahamcluley.com/in-its-ransomware-response-norsk-hydro-is-an-example-for-us-all> (дата звернення 14.01.2020).
22. Франция ищет в Украине хакеров, запустивших опасный вирус. URL: <https://www.internetua.com/franciya-isxet-v-ukraine-hakerov-zapustivshih-opasnyi-virus18> (дата звернення 14.01.2020).
23. EVIDENCE2e-CODEX. URL: <https://www.interpol.int/es/Quienes-somos/Marco-juridico/Information-communications-and-technology-ICT-law-projects/EVIDENCE2e-CODEX> (дата звернення 14.01.2020).
24. 11 Eye Opening Cyber Security Statistics for 2019. URL: <https://www.cpomagazine.com/tech/11-eye-opening-cyber-security-statistics-for-2019> (дата звернення 14.01.2020).
25. “Ми знайдемо людину навіть якщо є лише фото зі спини”: як стартап Traces AI розпізнає людей на відео без обличчя. URL: <https://www.epravda.com.ua/publications/2019/11/26/653992> (дата звернення 14.01.2020).

~~~~~ \* \* \* ~~~~~

УДК 342.52

ПЕТРОВ С.Г., кандидат юридичних наук.ORCID: <https://orcid.org/0000-0001-7786-4657>.

ОРГАНІЗАЦІЙНІ І ПРАВОВІ ОСНОВИ ВИРІШЕННЯ ПРОБЛЕМ ПРОТИДІЇ КІБЕРПОСЯГАННЯМ У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Анотація. У статті здійснено аналіз організаційних та правових підходів ЄС та окремих держав-членів щодо протидії кіберпосяганням. Запропоновано врахувати в Україні досвід Польщі щодо функціонування установи, яка поєднує наукові дослідження, освітні програми і практичну реалізацію заходів протидії кіберпосяганням, Австрії – щодо існування національного CERTу Австрії для приватного сектору.

Ключові слова: кіберпосягання, організаційні та правові основи, Європейський Союз, кібербезпека, державно-приватне партнерство.

Summary. The article deals with the issues of organizational and legal approaches of the EU and individual Member States to address cyber-attacks. It is suggested for Ukraine to take into account the experience of Poland in the functioning of an institution that combines scientific research, educational programs and practical implementation of measures against cyberattacks, of Austria – regarding the existence of a national CERT of Austria for the private sector

Keywords: cyber attacks, organizational and legal framework, European Union, cybersecurity, public-private partnership.

Аннотация. В статье осуществлен анализ организационных и правовых подходов ЕС и отдельных государств-членов по противодействию киберпосягательствам. Предложено учесть в Украине опыт Польши по функционированию учреждения, которое сочетает научные исследования, образовательные программы и практическую реализацию мер противодействия киберпосягательствам, Австрии – относительно существования национального CERT для частного сектора.

Ключевые слова: киберпосягательства, организационные и правовые основы, Европейский Союз, кибербезопасность, государственно-частное партнерство.

Постановка проблеми. Євроінтеграційний вектор України, закріплений в Угоді про асоціацію між Україною та Європейським Союзом, є незмінним зовнішньополітичним пріоритетом нашої держави. Угода про асоціацію визначила такий формат відносин між Україною та ЄС, який став стратегічним орієнтиром соціально-економічних реформ в Україні, зокрема і у безпековому напрямку.

Проблема захисту від кіберпосягань на інформаційні ресурси наразі є актуальною як для ЄС та його держав-членів, так і для України. Розбудова державних структур, поглиблення державно-приватного партнерства, удосконалення правових основ протидії кіберпосяганням вимагає усебічного аналізу позитивних практик провідних країн. Унікальність прикладів у цьому контексті полягає у дворівневому правовому регулюванні і відповідно управлінні: на рівні ЄС і на рівні держав-членів об'єднання.

Результати аналізу наукових публікацій свідчать про те, що питання забезпечення кібернетичної і інформаційної безпеки держави були предметом досліджень багатьох українських учених, а саме О.Д. Довганя, О.О. Климчука, А.І. Марущака, В.В. Остроухова, В.М. Панченко, В.Г. Пилипчука, В.І. Польового, О.Б. Розвадовського, В.Б. Хлевицького, О.М. Юрченка та інших.

Частково досвід країн-учасниць НАТО у сфері забезпечення кібернетичної безпеки розкривав Р.В.Лук'янчук, який акцентував увагу на етапах взаємодії між Україною та Альянсом у межах функціонування Трастового фонду НАТО з кібербезпеки, обґрунтував доцільність прискорення процесу приєднання України до НАТО з метою входження до системи колективної безпеки, у тому числі й у форматі забезпечення кібербезпеки [1].

Проблеми кібербезпеки останнім часом є предметом для обговорення на різноманітних науко-практичних форумах [2; 3]. Видаються підручники, які розкривають теоретичні та прикладні питання міжнародної інформаційної та кібербезпеки як складової міжнародної системи підтримання миру і стабільності [4].

На основі аналізу європейського досвіду з питань боротьби з правопорушеннями в інформаційній сфері дослідники обґрунтовують також часткові питання задля протидії кіберпосяганням, наприклад, необхідність підписання Меморандуму про взаєморозуміння між Інтернет-провайдерами та правоохоронними органами у межах державно-приватного партнерства [5].

Загалом, як бачимо, підходи Європейського Союзу і держав-членів до вирішення проблем протидії кіберпосяганням були предметом досліджень тільки частково.

Метою статті є розкриття організаційних і правових основ протидії кіберпосяганням у Європейському Союзі і формулювання прийнятних для України прикладів.

Виклад основного матеріалу. Розпочнемо з аналізу організаційних та правових підходів ЄС до спільної політики безпеки та оборони, які ґрунтуються на Глобальній стратегії щодо безпеки і оборони Європейського Союзу [6], Глобальній стратегії щодо зовнішніх відносин та безпеки Європейського Союзу [7] Плані реалізації Глобальної стратегії у сфері безпеки і оборони [8]. Зазначеними документами не тільки наголошується на важливості співробітництва ЄС і НАТО, а й на протидії гібридним загрозам, оперативному співробітництві з питань кібербезпеки.

Правову основу для протидії кіберпосяганням у Європейському Союзі безпосередньо визначає Будапештська Конвенція Ради Європи з кіберзлочинності (далі – Конвенція), прийнята ще у 2001 році [9], учасниками якої є не тільки країни Європи, а й інші (США, Аргентина, Австралія, Чилі, Японія та інші).

З метою розслідування або переслідування кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання електронних доказів, які стосуються кримінальних правопорушень, Конвенція передбачає загальні принципи міжнародного співробітництва, зокрема цілодобову інформаційну мережу національних контактних пунктів “24/7” для боротьби зі злочинами у сфері комп'ютерних технологій [9, ст.ст. 23, 35]. Така мережа забезпечує надання оперативної міжнародної правової допомоги, а саме термінове збереження комп'ютерних даних, щодо яких є загроза їх втрати, знищення або модифікації; збирання і вилучення доказів в електронній формі у кримінальних справах про вчинення транснаціональних кіберзлочинів; отримання оперативної інформації щодо обставин вчинення транснаціональних кіберзлочинів; встановлення місцезнаходження осіб, підозрюваних у вчиненні транснаціональних кіберзлочинів; оперативний інформаційний обмін щодо збережених та отриманих даних між національними та іноземними правоохоронними органами.

Остання зустріч національних представників мережі контактних пунктів “24/7” у межах спільної програми Ради Європи і ЄС Глобальної протидії кіберзлочинності (Global Action on Cybercrime Extended, GLACY+) [10] відбулася 8 жовтня 2019 р. і стосувалася практичних аспектів взаємодії правоохоронних органів держав-підписантів Конвенції [11].

ЄС продовжує розбудовувати інституційну платформу для обговорення актуальних питань кібербезпеки, боротьби з кіберзлочинністю тощо. Зокрема, на напрацювання єдиної міжнародної політики у сфері протидії кіберзлочинності у контексті перетворення Конвенції на єдиний міжнародний механізм спрямовується робота Програмного офісу з протидії кіберзлочинності Ради Європи – Cybercrime Programme Office (C-PROC) [12]. Одним з важливих питань, на яке спрямовуються зусилля фахівців C-PROC, є підвищення ефективності процедур правової допомоги при здійсненні заходів з протидії кіберзлочинності та кібертероризму. Комітетом Конвенції ще у червні 2017 року прийнято рішення щодо доцільності укладання додаткового протоколу до Конвенції з метою закріплення правових та організаційних передумов для створення спільних слідчих робочих груп з розслідування кіберзлочинів, міждержавної взаємодії із провайдерами Інтернет-послуг тощо.

Задля створення організаційних передумов для проведення спільних розслідувань кіберзлочинів у 2013 році в ЄС у складі Європолу створено Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre (EC3)) [13]. Основними завданнями EC3 передбачено: забезпечення обміну інформацією між підрозділами правоохоронних органів ЄС та третіми країнами; боротьба з розповсюдженням у мережі Інтернет дитячої порнографії; підготовка кваліфікованих кадрів у сфері боротьби з кіберзлочинністю; розробка методики виявлення і припинення злочинів у сфері інформаційних технологій тощо. Своєрідною “підслідністю” EC3 є кіберзлочини, які: скоєні міжнародними злочинними угрупованнями з метою отримання значних прибутків, або у результаті діяльності яких було задано значної шкоди; завдають значної шкоди потерпілим, зокрема, кібернасильство, сексуальна експлуатація дітей он-лайн, розповсюдження порнографії тощо; завдають шкоди критичній інфраструктурі країн-членів ЄС.

Вітчизняні дослідники інформаційно-правової науки, розкриваючи питання врахування європейського досвіду щодо питань боротьби з правопорушеннями в інформаційній сфері, обґрунтовують необхідність забезпечення доступу правоохоронних органів України їх до баз даних та аналітичних матеріалів Центру EC3 [5, с. 17]. Така позиція потребує підтримки з урахуванням того, що лише оперативний облік інформації є запорукою ефективності протидії кіберзлочинності. Відзначимо, що бажано забезпечувати доступ до зазначених ресурсів не лише Національній поліції України, а й інших правоохоронних органів, зокрема СБ України і Державного бюро розслідувань України.

Перейдемо до розгляду організаційних і правових основ для вирішення проблем протидії кіберпосяганням у окремих державах-членах ЄС. Розпочнемо з Федеративної Республіки Німеччини.

Оновлена Стратегія кібербезпеки ФРН від 9 листопада 2016 року удосконалює Стратегію кібербезпеки від 2011 року і передбачає понад 30 стратегічних цілей та заходів, зокрема спрямована на просвітницьку діяльність щодо роз'яснення важливості кібербезпеки для користувачів, розширення співпраці між державою та бізнесом, а також розширення мережі “команд швидкого реагування” на кіберзагрози [14].

У ФРН створено Національний центр кіберзахисту, який забезпечує ефективну співпрацю між усіма державними установами для координації захисних та контрзаходів щодо кіберінцидентів [15]. Зазначена платформа для співпраці об'єднує представників Федерального управління кримінальної поліції, Федерального управління з питань захисту Конституції, Федеральної служби розвідки, Федеральних Збройних Сил, Федерального управління з питань цивільного захисту та ліквідації наслідків

надзвичайних подій, Управління митної кримінальної поліції та контролюючий орган щодо операторів та критичних інформаційних інфраструктур – Федеральне відомство з питань інформаційної безпеки (далі – BSI).

Вітчизняні дослідники міжнародного права зазначають, що швидкий і вузьковідомчий обмін інформацією про вразливі місця ІТ-продуктів, форми нападу і злочинців надає можливість Національному центру кіберзахисту ФРН аналізувати кібератаки і давати узгоджені рекомендації щодо протидії [16].

У цьому контексті відзначимо, що в Україні продовжується робота щодо врахування провідного європейського досвіду у питаннях протидії кіберзагрозам. Зокрема, по аналогії з Національним центром кіберзахисту ФРН підвищено роль Національного координаційного центру кібербезпеки України (далі – НКЦК) відповідним Указом Президента України від 28 січня 2020 року [17]. На нашу думку, такі додаткові повноваження НКЦК, як здійснення координації та контролю за діяльністю суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, здійснення аналізу стану кіберзахисту критично важливих об'єктів інфраструктури, стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам, здійснення превентивних заходів у боротьбі з кіберзлочинністю; розроблення концептуальних засад і пропозицій щодо створення та функціонування відповідно до уніфікованих технічних вимог центрів обробки даних та центрів забезпечення кібербезпеки державних органів, а також об'єктів критичної інформаційної інфраструктури, упровадження вітчизняних програмних та програмно-апаратних засобів для здійснення уповноваженими суб'єктами заходів із кіберрозвідки, кібероборони, контррозвідувального захисту кібербезпеки держави, розслідування кіберзлочинів тощо стануть важливою передумовою централізації державної політики у сфері кібербезпеки.

Метою BSI є сприяння безпеці інформаційних технологій в Німеччині. BSI насамперед забезпечує кібербезпеку федерального уряду Німеччини, однак також пропонує свої послуги приватним та комерційним користувачам та постачальникам інформаційних технологій і запроваджує дієві технології приватно-публічного партнерства [18].

Заслугує на увагу також досвід Польщі у протидії кіберпосяганням, який свідчить про важливість стратегії, нормативних актів, впровадження їх в життя, ведення підготовки фахівців у сфері кібербезпеки, а також контролю окремих установ, підприємств і громадян, міжнародної співпраці, а також безперервного розвитку в цій сфері [19].

Польща бере активну участь у реалізації політики ООН, НАТО та ЄС, а також на оперативному рівні співпрацює з Чехією, Словаччиною, Угорщиною та Австрією у межах Центральноєвропейської платформи кібербезпеки [20].

Досвід Польщі цікавий тим, що у цій країні створено Урядовий центр безпеки (далі – RCB) задля створення ефективної та всебічної системи антикризового управління [21]. RCB – це надвідомча структура, спрямована на оптимізацію та стандартизацію сприйняття загроз окремими урядовими відомствами з метою підвищення їх здатності вирішувати складні ситуації.

Відповідно до Закону Польщі від 2007 року про управління кризовими ситуаціями, до критичної інфраструктури віднесено: системи постачання енергії, палива та енергії, системи зв'язку, телекомунікаційні мережі, фінансові системи, системи харчування, водопостачання, охорони здоров'я, транспортні системи, системи порятунку, системи, що забезпечують безперервність діяльності державного управління, системи виробництва, зберігання та використання хімічних і радіоактивних речовин, включаючи

трубопроводи для небезпечних речовин. Важливо для врахування у розбудові правової основи для захисту критичної інфраструктури в Україні враховувати, що під критичною інфраструктурою у Польщі розуміють як фізичну, так і кібернетичну системи (включаючи об'єкти, споруди чи установки), необхідні для мінімальної роботи економіки та держави [22].

Цікавим для врахування Україною є приклад функціонування Національного науково-дослідного інституту Польщі (далі – NASK), яким керує Міністерство цифрових справ Польщі і основна функція якого – це забезпечення безпеки Інтернету. NASK – це польський національний реєстратор імен Інтернету в домені.pl; NASK керує центром стратегічного аналізу щодо кібербезпеки; команда швидкого реагування CERT Polska також діє в структурі NASK; у цій установі створена платформа для державно-приватного партнерства.

Крім того, NASK здійснює науково-дослідну діяльність у галузі безпеки, надійності та ефективності мереж ІКТ, зокрема CyberSecIdent, Cyberpark ENIGMA – проекти, присвячені питанням кібербезпеки, які запроваджені в цій установі. Академія NASK проводить унікальні тренінги для компаній та установ з акцентом на безпеку ІКТ, а також модерує програму ЄС Безпечний Інтернет, сприяючи безпечному використанню нових технологій та Інтернету серед дітей та молоді [23]. Як бачимо, зазначена установа є не тільки адміністративним органом щодо регулювання доменних імен, реагування на кіберінциденти тощо, а й платформою для широкомасштабних наукових та освітніх проектів. Такий досвід є актуальним для нашої держави, оскільки передбачає поєднання наукових підходів, освітніх програм і практичної реалізації заходів протидії кіберпосяганням.

У Австрії система протидії кіберпосяганням ґрунтується на двох основних документах: Програмі захисту критичної інфраструктури (далі – APCIP) та Національній стратегії кіберзахисту.

Австрія має ефективну інфраструктуру і високий рівень безпеки постачання продовольства, транспорту, телекомунікацій, енергетичних та фінансових послуг, соціальних та медичних послуг. APCIP постійно доповнюється з метою забезпечення високої якості послуг і безпеки їх надання. Крім того, у Австрії Федеральною канцелярією започаткована “Платформа кібербезпеки” як основа для державно-приватного партнерства у сфері кібербезпеки та захисту критичної інфраструктури [24].

Національна стратегія з питань кібербезпеки передбачає, що забезпечення кібербезпеки в національному та міжнародному кіберпросторі є одним із головних пріоритетів Австрії та спільним викликом для держави, бізнесу та суспільства. З метою забезпечення регулярного обміну інформацією між зацікавленими сторонами в Австрії налагоджено постійний моніторинг та оцінка ситуації в кіберпросторі та запис відповідної інформації. Для забезпечення високої стійкості критичної інфраструктури проти кібератак створена Державна комп'ютерна команда реагування на надзвичайні ситуації, що управляється Федеральною канцелярією (GovCERT), а також, що є цікавим для України досвідом, CERT.at – національний CERT для приватного сектору Австрії.

Особливістю цієї установи є те, що вона координує реагування на кіберінциденти для недержавних підприємств та організацій, розглядаючи будь-яку інформацію, передану як конфіденційну інформацію, і не передаючи її без згоди, якщо тільки це явно не потрібно для оперативного реагування на інцидент (Національний CERT для приватного сектору Австрії – <https://cert.at/de/ueber-uns/zustaendigkeit>). Такий приклад вартий уваги для наслідування в Україні, оскільки вирішує питання недовіри приватних суб'єктів до державних установ та знижує їх репутаційні ризики.

Висновки.

Підсумовуючи викладене, зазначимо, що на основі аналізу організаційних та правових підходів ЄС до політики безпеки у сфері кіберпростору відзначено низку актуальних для України прикладів. Зокрема, відзначено активність Програмного офісу з протидії кіберзлочинності Ради Європи – Cybercrime Programme Office (C-PROC), який робить спробу закріпити правові та організаційні передумови для створення спільних слідчих робочих груп з розслідування кіберзлочинів, міждержавної взаємодії із провайдерами Інтернет-послуг тощо. Підтверджено наукову позицію щодо необхідності забезпечення доступу до ресурсів ЕСЗ широкого кола вітчизняних правоохоронних органів, зокрема СБ України і Державного бюро розслідувань України.

Аналіз організаційних і правових основ для вирішення проблем протидії кіберпосяганням у окремих державах-членах ЄС дав підстави для формулювання наступних висновків. Подібно до Національного центру кіберзахисту ФРН в Україні на початку 2020 року підвищено роль та повноваження НКЦК, що є важливою передумовою централізації державної політики у сфері кібербезпеки.

Актуальним для України є досвід Польщі у частині створення RCB – надвідомчої структури, спрямованої на оптимізацію та стандартизацію сприйняття загроз урядовими відомствами з метою підвищення їх здатності вирішувати складні ситуації, зокрема і у сфері захисту критичної інфраструктури, куди включено і кібернетичну систему.

Особливої уваги заслуговує приклад функціонування NASK Польщі, на базі якого поєднано наукові дослідження, освітні програми і практичну реалізацію заходів протидії кіберпосяганням.

Досвід Австрії заслуговує на врахування в Україні у частині державно-приватного партнерства у сфері кібербезпеки та захисту критичної інфраструктури, а саме існування національного CERTу Австрії для приватного сектору, що дає можливість вирішити питання недовіри приватних суб'єктів до державних установ та знижує їх репутаційні ризики.

Перспективами подальших досліджень визначаємо питання дослідження досвіду країн Азії у протидії кіберпосяганням.

Використана література

1. Лук'яничук Р.В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісн. Нац. акад. держ. упр. при Президентові України*. 2015. № 4. С. 50-56.
2. Міжнародні стандарти з кібербезпеки та їх застосування в Україні: мат-ли “круглого столу”, м. Харків, 19 квіт. 2016 р. / ред.: А.П. Гетьман, Б.М. Головкін. – (Нац. юрид. ун-т ім. Ярослава Мудрого). Харків: Право, 2016. 87 с.
3. Кримінальні загрози в секторі безпеки: практики ефективного реагування: мат-ли панельної дискусії III Харків. міжнар. юридичного форуму, м. Харків, 26 вересня 2019 р. – (Нац. юрид. ун-т ім. Ярослава Мудрого). Харків: Право, 2019. 172 с.
4. Міжнародна інформаційна безпека: теорія і практика: підруч. для студентів ВНЗ, які навчаються за напрямом підгот. “Міжнародні відносини” та “Міжнародна інформація” / Є.А.Макаренко, М.М. Рижков, М.А. Ожеван, О.П. Кучмій, О.М. Фролова. – (Нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин). Київ: Центр вільної преси, 2016. 417 с.
5. Марущак А.І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. *Безпека інформації*. 2019. Т. 25. № 1. С. 13-17.
6. Council conclusions on implementing the EU global strategy in the area of security and defence. URL: <https://www.consilium.europa.eu/en/press/press-releases/2016/11/14/conclusions-eu-global-strategy-security-defence>

7. EU global strategy on foreign and security policy. URL: http://www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf
8. Implementation Plan on Security and Defence. URL: <https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf>
9. Про кіберзлочинність: Конвенція Ради Європи від 21 листопада 2001 р. URL: http://www.zakon4.rada.gov.ua/laws/show/994_575
10. Global Action on Cybercrime Extended. URL: <https://www.coe.int/en/web/cybercrime/glacypus>
11. GLACY+ Third Annual Meeting of the 24/7 Network of Contact Points. URL: <https://www.coe.int/en/web/cybercrime/glacypusactivities>
12. Cybercrime Programme Office. URL: <https://www.coe.int/en/web/cybercrime/cybercrime-office-c-proc->
13. European Cybercrime Centre. URL: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>
14. Cyber-Sicherheitsstrategie für Deutschland 2016. URL: <http://www.bmi.bund.de/cybersicherheitsstrategie>.
15. Nationales CyberAbwehrzentrum. URL: https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html
16. Добржанська О.Л. Демцов А.А. Кібербезпека як феномен міжнародних відносин на прикладі Федеративної Республіки Німеччини. *Актуальні проблеми міжнародних відносин*. 2011. Вип. 102(1). С. 111-116.
17. Про внесення змін до Указів Президента України від 27 січня 2015 року № 37 та від 7 червня 2016 року № 242: Указ Президента України № 27/2020. URL: <https://www.president.gov.ua/documents/272020-32041>
18. Das Bundesamt für Sicherheit in der Informationstechnik. URL: <https://www.bsi.bund.de>
19. Сайт ENISA – (Агентство ЄС з кібербезпеки). URL: <https://www.enisa.europa.eu/topics/national-cyber-security-strategies>
20. Урядовий центр безпеки Польщі. URL: <https://www.rcb.gov.pl/en/about-us>
21. Critical infrastructure. URL: <https://www.rcb.gov.pl/en/critical-infrastructure>
22. Національний науково-дослідний інститут Польщі. URL: <https://www.eng.nask.pl>
23. Програма захисту критичної інфраструктури Австрії (APCIP). URL: <https://www.bundeskanzleramt.gv.at/themen/sicherheitspolitik/schutz-kritischer-infrastrukturen.html>

~~~~~ \* \* \* ~~~~~

УДК 659.3(477)

ДОРОГИХ С.О., кандидат юридичних наук, с.н.с., НДІП НАПрН України.  
ORCID: <https://orcid.org/0000-0002-2748-1938>.

## ЗАЛУЧЕННЯ ГРОМАДЯН ДО ЗАКОНОТВОРЧОГО ПРОЦЕСУ: ДЕЯКІ ПІДСУМКИ

**Анотація.** Розглядаються деякі аспекти практичної реалізації залучення громадян до законотворчого процесу.

**Ключові слова:** інформаційна діяльність, парламент, електронний парламент, електронні петиції.

**Summary.** Some aspects of practical implementation of citizen involvement in the legislative process are considered.

**Keyword:** information activities, parliament, e-parliament, electronic petitions.

**Аннотация.** Рассматриваются некоторые аспекты практического привлечения граждан к работе парламента.

**Ключевые слова:** информационная деятельность, парламент, электронный парламент, электронные петиции.

**Постановка проблеми.** Розвиток громадянського суспільства вимагає впровадження контролю з боку суспільства за діяльністю влади. Україна намагається вирішити це питання через дотримання принципів відкритості та прозорості діяльності всіх гілок влади. У монографії “Забезпечення принципів відкритості та прозорості в інформаційній діяльності Верховної Ради України” [1] розглядалися теоретичні питання такої діяльності у законодавчій гілці влади. Вважаємо за необхідне розглянути як це реалізовано на практиці й проаналізувати як досягнення, так і виявленні проблеми.

**Метою статті** є оцінка практичної реалізації процесу залучення громадян до законотворчого процесу.

**Виклад основних положень.** Співпраця державних органів з громадянським суспільством створює необхідну передумову для створення зворотного зв'язку, без якого неможливе ефективне державне управління.

Дотримання принципів відкритості та прозорості у діяльності законодавчої гілки влади призвело до впровадження на офіційному веб-порталі Верховної Ради України “Особистого кабінету громадянина”.

На сьогодні “Особистий кабінет громадянина” дозволяє надіслати звернення, прийняти участь із обговорення законопроектів, створити електронну петицію та віддати голос за вже існуючу, записатися на відвідання відкритого пленарного засідання Верховної Ради України, а також перейти до порталу відкритих даних та бази даних нормативно-правових актів України.

Як же працюють ці механізми на практиці? Почнемо з процесу обговорення законопроектів.

Метою створення механізму он-лайн обговорення законопроектів було залучення фахівців до кваліфікованого громадського обговорення законопроектів для підвищення їх якості, побудови зворотного зв'язку між громадянами та депутатами, врахування інтересів широких верств населення. Що ми отримали у підсумку? На жаль дуже мало.

Необхідність обговорення громадянами законопроектів була затверджена у “Плані дій з реалізації Декларації відкритості парламенту” [2]. Зокрема у Плані передбачалося внести зміни до Регламенту Верховної Ради України та відповідно забезпечити права громадян України:

- коментувати окремі положення законопроектів та законопроекти в цілому на веб-сайтах комітетів у розділі “Законопроекти, винесені на обговорення”;
- коментувати окремі положення та законопроекти в цілому безпосередньо на їх сторінках (картка законопроекту);
- відслідковувати результат розгляду та врахування їх коментарів та пропозицій.

Крім того, необхідно було доповнити текст порівняльної таблиці “Результати громадського обговорення законопроекту”, підготовленої до опрацювання законопроекту комітетами Верховної Ради України.

З вище перерахованих пунктів було реалізовано тільки можливість коментувати окремі законопроекти в цілому.

Станом на початок березня 2020 року було обговорено за даними веб-сайту Верховної Ради України 25 законопроектів, до яких громадяни могли подавати зауваження та пропозиції та надсилати коментарі. За обсягом обговорення на першому місці був проект Закону про цивільну зброю і боєприпаси за № 1135-1. До нього було подано 61 пропозиція, з яких враховано – 0. Така сама ситуація й з іншими обговореннями законопроектів. За часів останнього складу Верховної Ради процес обговорення законопроектів повністю припинився (останнє обговорення закінчилося у жовтні 2019 року).

Як ми бачимо, жодна з пропозицій не була прийнята, що у подальшому буде демотивувати громадян подавати якісні пропозиції до законопроектів.

На жаль на сьогодні у Регламенті Верховної Ради України не врегульовані як процедура коментування законопроектів громадянами, так і процедура врахування чи розгляду зауважень громадян законотворцями. Це призводить до того, що пропозиції громадян не тільки не обговорюються, а з ними навіть не знайомляться, що значно зменшує мотивування громадян до участі у законотворчій роботі.

Окрім цього, на мотивування громадян до законотворчої діяльності безпосередньо буде впливати чи беруть участь у обговоренні депутати, їх помічники, експерти Верховної Ради та профільних Міністерств. Поки що ми цього не бачимо. Тобто принципи розвитку парламентаризму, які вимагають дотримання стандартів відкритості та прозорості, у тому числі за рахунок спілкування депутатів з громадськістю, залучення як фахового середовища, так і окремих громадян і громадських організацій до обговорення законопроектів на словах підтримуються, а на практиці – не працюють.

На сьогодні обговорення законопроектів практично припинено.

Як можливо змінити ситуацію на краще?

По-перше, це дотримання усіх пунктів Плану дій з реалізації Декларації відкритості парламенту.

По-друге, це залучення наукової та фахової спільноти до обговорення законопроектів.

Дещо краще йдуть справи з впровадженням електронних петицій.

28 жовтня 2015 р. Верховною Радою було прийнято Закон України “Про внесення змін до Закону України “Про звернення громадян” щодо електронного звернення та електронних петицій” [3], у якому громадянам надається право подавати електронні петиції, в тому числі до Верховної Ради України. Згідно цього Закону за результатами розгляду електронної петиції народними депутатами України можуть розроблятися та вноситися в установленому порядку на розгляд Верховної Ради України законопроекти, спрямовані на вирішення порушених у петиції питань.

Згідно з прийнятим Законом Голова Верховної Ради не пізніше трьох робочих днів після отримання електронної петиції направляє її в комітет, який відповідно до предмета відання визначається головним з підготовки і попереднього розгляду електронної петиції. Головний комітет не пізніше десяти робочих днів після отримання електронної петиції розглядає її на своєму засіданні. На засідання головного комітету запрошується автор (ініціатор) електронної петиції, а в разі необхідності – представники Кабінету Міністрів України, міністерств, інших державних органів, об'єднань громадян, а також експерти, фахівці та інші особи.

Головний комітет затверджує висновок про результати розгляду питань, що порушуються в електронній петиції, а також у разі необхідності готує проект відповідного акта Верховної Ради. А у разі наявності в електронній петиції клопотання про проведення парламентських слухань, комітет готує відповідний проект постанови Верховної Ради та подає його в порядку, визначеному цим Законом.

Висновок головного комітету та проект акта Верховної Ради, підготовлений головним комітетом, без прийняття рішення про включення до порядку денного пленарного засідання Верховної Ради обговорюється за процедурою повного обговорення на наступному після дня внесення пленарному засіданні Верховної Ради.

Незважаючи на те, що прийнятий закон має ряд вад, на які цілком слушно вказує Головне юридичне управління Верховної Ради України (приміром, щодо встановлення відповідальності “за зміст електронної петиції”, а також з приводу законодавчого визначення поняття “офіційний веб-сайт”) [4], що вказує на необхідність досконалого опрацювання питання використання механізмів електронної петиції у вітчизняному законодавстві, сам напрям розвитку залучення громадян до законотворчої роботи заслуговує уваги та подальшої розробки.

У подальшому система електронних петицій може бути інтегрована як до електронного документообігу у парламенті, так і до загальної системи “електронного парламенту” як комплексу баз даних, програмного забезпечення та технічних засобів, створених для підтримки всіх стадій законотворчого процесу, забезпечення доступу громадян до публічної інформації та організації спілкування між громадянами, парламентом та депутатами.

На сьогодні вже функціонує веб-портал “Електронні петиції Верховної Ради України”, який розташовано за адресою: <https://itd.rada.gov.ua/services/Petitions>.

Станом на кінець січня 2020 року було подано 152 петицій. З них 12 петицій набрали 25000 голосів на свою підтримку. Так ряд петицій отримали підтримку відповідних профільних комітетів. Так, наприклад, петиція “Вони живі, вони все відчувають, у них є душа. Заборонити тестування косметики на тваринах” отримала схвальну реакцію Комітету з питань екологічної політики та природокористування та пропозицію до Міністерства охорони здоров'я внести до 1 лютого 2020 року до Кабінету міністрів України проект технічного регламенту про косметичну продукцію, яка відповідає Регламенту (ЄС) № 1223/2009 Європейського Парламенту та Ради на косметичну продукцію, що розміщується на внутрішньому ринку ЄС. Кабінету Міністрів рекомендується розробити та затвердити план заходів із впровадження технічного регламенту на косметичну продукцію.

Обговорення пропозицій, наданих у петиції “Захист дітей від сексуального насильства” було включено до порядку денного Верховної Ради, а пропозиції, які були сформульовані у петиції “Вимагаємо повернути залізничникам, які безпосередньо здійснюють організацію залізничних перевезень та забезпечують безпеку руху поїздів, право дострокового виходу на пенсію за вислугу років”, профільний комітет рекомендував розглянути й прийняти за основу у відповідному законопроекті.

Не всі петиції, які набрали 25000 голосів на свою підтримку, отримали схвальні відгуки. Рішення деяких питань було переадресовано до Кабінету Міністрів, а у деяких петиціях пропозиції авторів носили яскраво виражений емоційний характер й не могли бути вирішені простим прийняттям певного законопроекту чи взагалі не відповідали законам України та міжнародним договорам, ратифікованим Україною, як, наприклад, петиція “Просимо вжити заходів для припинення пропаганди гомосексуалізму та захисту традиційних сімейних цінностей”.

У чому полягає відмінність механізмів обговорення законопроектів та електронних петицій? Чому один механізм працює, а інший – ні? Відповідь у законодавчо закріпленій процедурі. Якщо процедуру внесення, реєстрації та розгляду електронної петиції прописано у відповідному Законі, то обговорення законопроектів зведено до факультативного написання коментарів, на які просто не зважають у законотворчому процесі.

Що стосується таких опцій як “Портал відкритих даних” та “Законодавство України”, то завдяки спільній роботі Апарату Верховної Ради на Науково-дослідного інституту інформатики і права НАПрН України, будь-який громадянин України, який має доступ до мережі Інтернет, має доступ до безкоштовної повної бази даних нормативно-правових актів України, а завдяки Порталу відкритих даних певні бази даних можна отримати для швидкої машинної обробки та аналізу.

### **Висновки.**

Хоча Україна й має значні досягнення у вирішенні питань дотримання принципів прозорості і доступу до публічної інформації щодо роботи парламенту, але розв’язання питань, пов’язаних із залученням громадськості до законотворчої роботи, існує лише у окремих проектах та потребує подальшого вдосконалення.

І якщо система електронних петицій працює, то, на нашу думку, побудова системи обговорення законопроектів потребує повного переосмислення.

Зазначимо, що повноцінне залучення громадян до законотворчого процесу можливо тільки за умови реального врахування пропозицій громадян у законопроектній роботі та розгляд їх у робочих комітетах. Відповідно потрібна детально розроблена й затверджена у Регламенті Верховної Ради України процедура надання, реєстрації та обговорення пропозицій, наданих громадянами, науковими та громадськими організаціями.

### **Використана література**

1. Дорогих С.О. Відкритість та прозорість в інформаційній діяльності Верховної Ради України: організаційно-правові аспекти: монографія. Київ: Видавничий дім “АртЕк”. 2018. 160 с.
2. Про деякі заходи щодо забезпечення відкритості процесу роботи Верховної Ради України, її органів, народних депутатів України та Апарату Верховної Ради України: Розпорядження Голови Верховної Ради України від 05.02.16 р. № 15. URL: <http://www.zakon.rada.gov.ua>
3. Про звернення громадян : Закон України від 02.10.1996 № 393/96-ВР. URL: <http://zakon.rada.gov.ua>
4. Зауваження до проекту Закону України “Про внесення змін до Закону України “Про звернення громадян” щодо електронного звернення та електронної петиції” (реєстр № 2299). – (Головне юридичне управління Верховної Ради України). URL: <http://www.rada.gov.ua>

~~~~~ \* \* \* ~~~~~

УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., доктор юридичних наук, с.н.с., головний науковий співробітник
НДІ інформатики і права НАПрН України.
ORCID: <https://orcid.org/0000-0003-3879-2237>.

КОНЦЕПТУАЛЬНА МОДЕЛЬ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ ЗАСОБАМИ КРИМІНАЛЬНОГО ПРАВА

Анотація. У статті обґрунтовується необхідність створення чіткої несуперечливої концептуальної моделі кримінально-правового захисту інформаційного простору Української держави та внесення у зв'язку із цим змін та доповнень до чинного Кримінального кодексу України.

Ключові слова: інформаційний простір, інформаційна безпека, інформаційні відносини, інформаційні злочини, кібербезпека.

Summary. The article substantiates the need to create a clear and consistent conceptual model of criminal legal protection of the information space of the Ukrainian state and to make changes and additions to the current Criminal code of Ukraine in this regard.

Keywords: information space, information security, information relations, information crimes, cybersecurity.

Аннотация. В статье обосновывается необходимость создания четкой непротиворечивой концептуальной модели уголовно-правовой защиты информационного пространства Украинского государства и внесения в связи с этим изменений и дополнений в действующий Уголовный кодекс Украины.

Ключевые слова: информационное пространство, информационная безопасность, информационные отношения, информационные преступления, кибербезопасность.

Постановка проблеми. Для якомога кращого розуміння феномену глобалізації сучасного світу та його проблем виникає потреба в осмисленні цього світу як єдиної системи комунікативних зв'язків, що стає можливим завдяки стрімкому розвитку й запровадженню інформаційних технологій у життєдіяльність суспільства та переходу останнього в якісно нову фазу свого розвитку – інформаційну. Одними із наочних проявів цього процесу є не лише поступове нівелювання значення фізичних кордонів між державами, які дедалі сприйматимуться не більше, ніж умовністю, даниною часу, а й епоха тотального панування інформаційного простору з усіма негативними та позитивними наслідками, що випливають із цього факту. Перед деякими із негативних аспектів інформаційного простору людина, суспільство та держава виявляються протягом якогось часу ледве чи небеззахисними, адже під впливом інформаційної глобалістики інколи створюються такі загрози переліченим фундаментальним категоріям, які піддаються правовій оцінці “із запізненням”, а тому про ніяку своєчасність реагування на них, на жаль, не може йтися, хоча відповідно до ст. 17 Конституції України забезпечення інформаційної безпеки України є однією з найважливіших функцій держави. Тому недаремно парною для категорії “інформаційний простір” стає саме категорія “інформаційна безпека”, визначень якої на теперішній час безліч. Не вдаючись до дискусії про повноту охоплення подібними визначеннями усіх сенсоутворюючих рис описаного явища, лише зазначимо, що, по-перше, безпека інформаційна від другої половини ХХ ст. стає одним із найважливіших елементів національної безпеки [1, с. 74], адже вона є невід’ємною частиною, яка

входить до інших складових національної безпеки, таких як економічна, воєнна, політична, екологічна, науково-технологічна тощо, а, по-друге, існування й реалізація багатьох загроз у цій сфері вже на теперішній час кваліфікуються як правопорушення з відповідними правовими наслідками, що тягне їх вчинення. Причому із розвитком інформаційного суспільства відбувається збільшення кількості порушень правових норм, що регулюють інформаційні відносини [2, с. 56]. Свого часу раніше чинний Закон України “Про основи національної безпеки України” від 2003 р. у ст. 7 визначав, що до головних реальних і потенційних загроз національним інтересам і національній безпеці України в інформаційній сфері належать: прояви обмеження свободи слова та доступу до публічної інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну таємницю, або іншої інформації з обмеженим доступом, спрямованої на задоволення потреб і забезпечення захисту національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [3]*. У 2015 р. у нашій державі прийнято Стратегію національної безпеки України, в якій до актуальних загроз саме інформаційній безпеці віднесено: ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства (п. 3.6). Що стосується загроз кібербезпеці і безпеці інформаційних ресурсів, то до їх числа належать: уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом (п. 3.7) [5]. Не дивлячись на спробу визначитися з основними загрозами розглядуваній сфері, слід відзначити, що стосовно деяких явищ, що мають, безумовно, шкідливий характер, законодавець й досі у роздумі. Висловлене, наприклад, стосується винайдення все нових і нових форм здійснення як масштабного психологічного впливу на населення, що мешкає на певній території (особливо в умовах ведення так званих гібридних війн), так і впливу, мішенню якого стають окремі люди або групи людей (стокерство, мобінг, булінг, хейзинг та ін.). Крім того, конче потрібна реакція держави на випадки навмисного приховування або необґрунтованої відмови посадових осіб від надання відповідної інформації чи надання інформації, що не відповідає дійсності; використання або(та) поширення інформації щодо особистого життя будь-якої особи без її згоди іншою особою, якій така інформація відома внаслідок виконання своїх службових обов’язків тощо. Так само не можна не звернути увагу на те, що через відсутність у чинному законодавстві України відповідальності за систематичне умисне поширення дезінформації наразі назріла потреба в принциповому обговоренні законопроекту “Про протидію дезінформації”, презентованого Міністерством культури, молоді та спорту України. Метою цього документа є захист інформаційного простору України від дезінформації та гібридних загроз із питань, які становлять суспільний інтерес і стосуються національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров’я громадян, довкілля тощо [6].

Проблематика розвитку й убезпечення інформаційного простору постійно знаходиться в зоні підвищеної уваги науковців і практиків. Різні аспекти захисту

* *Примітка.* У 2018 р. прийнято новий Закон України “Про національну безпеку України”, в якому окремо вже не наводиться перелік загроз інформаційній (кібернетичній) безпеці країни (див. [4]).

інформаційного простору України засобами кримінального права, у тому числі у контексті реалізації завдань із захисту національної безпеки, а так само питання створення ефективної системи запобіжних заходів від загроз у зазначеній сфері розроблялися такими вітчизняними вченими, як Д.С. Азаров, П.С. Берзін, М.В. Бутузов, В.Д. Гавловський, М.В. Карчевський, М.О. Кравцова, С.А. Кузьмін, О.М. Литвинов, В.В. Марков, А.І. Марущак, А.А. Музика, В.Г. Пилипчук, О.Е. Радутний, Н.А. Савінова, В.Б. Харченко, В.П. Шеломенцев та ін. Звісно ж, ці розробки ґрунтуються на доробках у галузі інформаційного права та правових засобів регулювання кіберпростору, найбільш значні з яких відображені у працях вітчизняних та зарубіжних вчених (О.А. Баранов, В.Ю. Баскаков, Дж. Голдсміт (J. Goldsmith) і Т. Ву (T. Wu), М.І. Дімчогло, В.М. Желіховський, М.З. Згуровський, Л.П. Коваленко, Б.А. Кормич, Л. Лессіг (L. Lessig), М. Лібіцкі (M.C. Libicki), В.А. Ліпкан, О.В. Логінов, Е. Лонгуорт (E. Longworth), В. Майер-Шонбергер (V. Mayer-Schunberger), Ю.Є. Максименко, О.А. Мандзюк, П.Є. Матвієнко, Г.М. Писаренко, Л.І. Рудник, В. І. Теремецький, Е. Тоффлер (A. Toffler), М. Цівіц (M. Ziewitz), В.С. Шапіро, О.В. Шепета та ін.

Проте висловлені ідеї у працях згаданих вище учених-правників здебільшого стосуються чи то розв'язання загальнотеоретичних проблем убезпечення інформаційного простору (насамперед кіберпростору) за допомогою правових механізмів цього захисту, чи то захисту інтересів особи, суспільства або держави від окремих видів правопорушень у розглядуваній сфері. Однак, коли триває напружена робота над новим Кримінальним кодексом України, природно виникає запитання про концептуальну модель кримінально-правового захисту інформаційного простору, що братиметься до уваги під час упорядкування норм про кримінальну відповідальність за злочини відповідної спрямованості. Тому є сенс звернутися до аналізу позицій із приводу забезпечення нормального функціонування інформаційного простору засобами, що за своєю природою виявляються *ultima ratio*.

Метою статті є: по-перше, аналіз нормативного матеріалу, за допомогою якого виконуються завдання закону про кримінальну відповідальність за правопорушення в інформаційному просторі України на теперішній час; по-друге, вибірковий огляд позицій, що висловлені з приводу захисту зазначеного сегмента життєдіяльності суспільства; по-третє, моделювання можливого підходу до організації правової матерії у сфері захисту інформаційного простору України від кримінально караних правопорушень.

Виклад основного матеріалу. На теперішній час відповідальність за порушення так званих інформаційно-правових норм передбачається у цивільно-правовому, адміністративному та кримінальному законодавстві. Так, за правопорушення в інформаційній сфері лише Кримінальним кодексом України встановлена відповідальність у кількох десятках статей. При цьому особливістю нинішньої моделі захисту інформаційних відносин є те, що відповідні норми містяться у різних розділах Особливої частини законодавства про кримінальну відповідальність. Однак важливо підкреслити, що розглядаючи питання відповідальності за протиправні діяння в інформаційному просторі, а так само криміналізуючи нові суспільно небезпечні діяння у цій сфері, йдеться не лише про кіберпростір як середовище, створюване інформаційними системами, об'єднаними в локальні або глобальні комп'ютерні мережі або реалізованими на окремих комп'ютерах та інших пристроях [7, с. 191], а й про циркуляцію будь-якої інформації, з використанням якої може пов'язуватися вчинення злочину.

Так би мовити, класичними прикладами порушення законодавства в інформаційному просторі є комп'ютерні злочини (розділ XVI Особливої частини КК

України), незаконне розголошення інформації з обмеженим доступом (наприклад, розголошення відомостей, що становлять державну або професійну (службову) таємницю, особою, якій ці відомості були довірені або стали відомі у зв'язку з виконанням службових або професійних обов'язків (статті 111, 132, 163, 168, 232, 384, 387 та ін. КК України) або, навпаки, приховування чи перекручування певних відомостей (інформації) (статті 220², 232², 238, 298¹ та ін. КК України)). Також важливе значення інформаційний вплив (інакше кажучи, певні дії в інформаційному просторі) на особу має і під час вчинення багатьох інших злочинів. Так, об'єктивна сторона доведення до самогубства може полягати у шантажі, тобто погрозі розголошення відомостей, які потерпілий бажає зберегти в таємниці [8, с. 53]. Шахрайство, в якому обман потерпілого здійснюється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (так звані комп'ютерні шахрайства), є наочним прикладом того, як "успіх" злочинних дій стає можливим завдяки інформаційному впливу на особу за допомогою інструментів кіберпростору. Як бачимо, низка статей КК України встановлює відповідальність за вчинення певних дій, що можуть мати значення для інформаційних відносин, хоча в диспозиціях таких статей про ці відносини й не згадується. Але тим не менш, повторимося, до орбіти протиправних дій "потрапляє" інформаційний простір, в якому потерпіла особа втрачає впевненість та починає відчувати себе в небезпеці, інколи вчиняючи будь-які дії, що, врешті-решт, завдають шкоду самій цій особі.

Якщо звернутися до Конвенції про кіберзлочинність 2001 р., підготовленої Радою Європи та ратифікованої Україною у 2005 р., із самої назви документа випливає, що правопорушення в інформаційному просторі цією Конвенцією обмежуються лише кіберпростором. Так, нею розрізняються чотири види кримінальних правопорушень:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, нелегальне перехоплення, втручання в дані та втручання в систему);

2) правопорушення, пов'язані з комп'ютерами (підробка та шахрайство, пов'язані з комп'ютерами);

3) правопорушення, пов'язані зі змістом (дитяча порнографія);

4) правопорушення, пов'язані з порушенням авторських та суміжних прав [9].

Отже, у цілому йдеться про загрози кібербезпеці, метою якої є виключно захист оброблюваних цифрових даних, на відміну від інформаційної безпеки в цілому, що призначена для комплексного захисту інформаційних ресурсів і даних у будь-якій формі.

Засновуючись на наведеній класифікації конвенційних правопорушень, О.В. Юрченко та О.Д. Дудченко наводять своєрідний атлас злочинів у сфері кібернетичної безпеки, одночасно доповнюючи перелік тих злочинів, що не віднесені Конвенцією до виокремлених груп правопорушень. Так, до групи злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем ними віднесено незаконний доступ (хакерство, злам шифру, інформаційний шпіонаж, перехоплення даних, спотворення інформації та систем). Група злочинів, пов'язаних із контекстом, може бути представлена такими діяннями, як виготовлення еротичних або порнографічних матеріалів, дитячої порнографії, расизм, агресивні висловлювання, релігійні злочини, наклеп і фальшива інформація. У свою чергу, до злочинів, пов'язаних із правом власності в інформаційній сфері, слід віднести злочини проти авторських прав, торгівельних знаків, незаконні азартні ігри, спам і пов'язані з ним загрози. До злочинів, пов'язаних із комп'ютерами, дослідниками віднесено шахрайство і

комп'ютерне шахрайство, підробка з використанням комп'ютера, крадіжка ідентичності, неправильне використання пристроїв. Окремо наводиться група так званих комбінованих злочинів, до яких належать, наприклад, кібертероризм, інформаційна війна, відмивання грошей із використанням комп'ютерних технологій, фітінг [10].

Як бачимо, чимало злочинів, зокрема так званої загальнокримінальної спрямованості й тих, що пов'язані з інформаційним впливом або поряд з іншим посягають і на інформаційний простір тріади “особа-суспільство-держава”, все одно залишаються поза межами цього своєрідного атласу, оскільки до уваги беруться лише діяння в кіберпросторі. До того ж перелічується чимало таких діянь, правова природа яких ще не має чіткого визначення (наприклад, фальшива інформація, інформаційна війна) або які на теперішній час не криміналізовані, хоча колись піддавалися захисту заходами кримінально-правового впливу (наприклад, наклеп). Водночас звернемо увагу на той факт, що запропонований підхід все ж таки можна визначити як спробу надання більш-менш систематизованого переліку діянь, що володіють ознакою суспільної небезпечності, посягаючи на інформаційний простір держави, суспільства та особи як такий.

У розвиток думки про суспільно небезпечні діяння, що реально існують, але ще не криміналізовані, окремо слід зупинитися на обговоренні ідеї про розробку і прийняття Закону України “Про протидію дезінформації”, представленого, як вже зазначалося, Міністерством культури, молоді та спорту України. Уявляється, що на теперішній час протидія дезінформації – одна з ключових проблем убезпечення національного інформаційного простору від загроз в умовах ведення так званої гібридної війни проти нашої держави, низького рівня медіаграмотності українців та неможливості ідентифікувати особу, яка масово розповсюджує ту чи іншу дезінформацію. Так, на сьогодні чинним законодавством України не передбачено можливості звернення до правоохоронних органів і суду з приводу поширення дезінформації за відсутності особи, чії права безпосередньо порушено. Не вдаючись до аналізу ідей, які запропоновано покласти в основу проєкту розглядуваного нормативного акта стосовно правових форм та організаційно-технічних методів ідентифікації осіб, що є поширювачами інформації, у тому числі й неправдивої, лише підкреслимо, що в чинному законодавстві України сьогодні відсутня відповідальність за масове поширення дезінформації в інформаційному просторі. Тому, враховуючи велику шкоду, що сягає рівня соціальної шкідливості або навіть суспільної небезпечності та може завдаватися такими діями одразу державі, суспільству та необмеженому колу осіб, є сенс встановлення, по-перше, адміністративної відповідальності за розповсюдження дезінформації, порушення правил спростування, надання відповіді та вимог прозорості, а по-друге, кримінальної відповідальності за систематичне умисне масове розповсюдження завідомо недостовірних повідомлень про факти, події або явища, що становить загрозу національній безпеці, громадській безпеці, територіальній цілісності, суверенітету, обороноздатності України, праву українського народу на самовизначення, життя та здоров'я громадян, стану довкілля у період відсутності повного контролю України за державним кордоном України. При цьому кваліфікуючими або особливо кваліфікуючими ознаками перелічених кримінально караних дій пропонується визнати їх вчинення з використанням комп'ютерних програм, призначених для автоматичного масового розповсюдження інформації (ботів), або спеціально організованої системи (групи) облікових записів, або користувачів інформаційних послуг, або засобів умисного фальшування (підробки) джерел інформації, а так само фінансування подібних

дій, вчинення їх повторно або організованою групою осіб, або якщо вони призвели до тяжких наслідків чи спричинили матеріальну шкоду у великому розмірі [11].

Надавши, але не вичерпавши доволі розлогу палітру правопорушень, що становлять безпосередню загрозу інформаційному простору, звернемося й до спроб розв'язати проблему створення оптимальної моделі захисту інформаційного простору за допомогою важелів кримінального права, що мали місце деякий час тому в національній площині. Так, ще наприкінці 2011 р. до Верховної Ради України було внесено проєкт Закону України “Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки” № 9575, що мав за мету вдосконалити систему юридичної відповідальності за правопорушення в сфері інформаційної безпеки. У цьому документі пропонувалося вилучити з КК України ст. 132 (Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби), ст. 145 (Незаконне розголошення лікарської таємниці), ст. 159 (Порушення таємниці голосування), ст. 163 (Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер), ст. 168 (Розголошення таємниці усиновлення (удочеріння)), ст. 182 (Порушення недоторканності приватного життя), ст. 231 (Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю), ст. 232 (Розголошення комерційної або банківської таємниці), ст. 328 (Розголошення державної таємниці), ст. 330 (Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни), ст. 376¹ (Незаконне втручання в роботу автоматизованої системи документообігу суду), ст. 381 (Розголошення відомостей про заходи безпеки щодо особи, взятої під захист), положення ст. 158 (Надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців) щодо втручання або інших несанкціонованих дій з базою даних та положення ст. 209¹ (Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму) у частині розголошення в будь-якому вигляді інформації, яка відповідно до закону надається спеціально уповноваженому центральному органу виконавчої влади зі спеціальним статусом із питань фінансового моніторингу, особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю, ст. 387 (Розголошення даних оперативно-розшукової діяльності, досудового розслідування), ч. 1 ст. 422 (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості). Натомість, запропоновано узагальнити та включити вилучені статті й склади злочинів до розділу XVI Особливої частини КК України, при цьому замінивши назву розділу “Злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку” на “Злочини у сфері інформаційної безпеки” [12].

На наш погляд, висловлена раніше позиція має рацію. Адже сфера інформаційної безпеки у широкому смислі слова виступає самостійним, дуже помітним об'єктом кримінально-правового захисту, який в умовах сьогодення потребує підвищеної уваги з огляду на необхідність забезпечення інформаційних відносин надійним захистом відповідного рівня та якості. Так, лише у 2019 р. за розділом XVI КК України зареєстровано 2088 злочинів. У свою чергу, за цей рік зафіксовано 210 випадків

порушення недоторканності приватного життя (ст. 182 КК України), що пов'язано зі збиранням, зберіганням, поширенням конфіденційної інформації про особу без її згоди або розголосом відомостей про особисту чи сімейну таємницю.

Повертаючись до структури КК України, зробимо висновок, що у чинному Кодексі з усього масиву злочинних діянь проти інформаційних відносин відповідного простору до Розділу XVI включені тільки ті з них, що пов'язані зі сферою кіберпростору (комп'ютерної інформації). Однак, на наш погляд, розмірковуючи над оптимальною моделлю захисту засобами кримінального права чисельних інформаційних відносин, що виникають й існують у суспільстві, треба виходити, по-перше, з акумуляції норм, що здійснюють захист усіх суб'єктів, яким може завдаватися шкода (особа, суспільство та держава) переважною більшістю відповідних злочинів, в одному розділі КК України, а, по-друге, доцільно вести мову не про захист інформаційних відносин у вузькому їх розумінні, а про захист інформаційного простору, під яким розуміється "інформаційне середовище, в якому відбуваються інформаційні процеси та інформаційні відносини щодо створення, збирання, одержання, зберігання, використання поширення, охорони та захисту інформації, інформаційних продуктів та інформаційних ресурсів" [7, с. 166]. Тобто йдеться про такий простір, що покликаний забезпечувати нормальну й безпечну інформаційну взаємодію між окремими особами, суспільством і державою у різних комбінаціях.

Таким чином, з урахуванням викладеної вище інформації та виходячи з наведеного розуміння інформаційного простору, вважаємо за доцільне здійснити оптимізацію кримінально-правового забезпечення охорони інформаційної безпеки України, насамперед змінивши назву розділу XVI Особливої частини КК України на таку: "Злочини проти інформаційної безпеки особи, суспільства, держави". При цьому до єдиного розділу кодексу слід віднести, по-перше, всі так звані комп'ютерні злочини, що містяться у теперішньому розділі XVI Особливої частини КК України (статті 361, 361¹, 361², 362, 363, 363¹), та злочини, пов'язані із внесенням неправдивих відомостей або будь-яким втручанням у роботу баз даних державних реєстрів (ст. 158 КК України (Надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців) у частині умисного внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованих дій з інформацією, що міститься в базі даних Державного реєстру виборців, чи іншого несанкціонованого втручання в роботу бази даних Державного реєстру виборців; ст. 376¹ (Незаконне втручання в роботу автоматизованої системи документообігу суду).

По-друге, до цього ж самого Розділу логічно перемістити склади злочинів, що на теперішній час містяться в інших розділах КК України, але стосуються однієї специфічної площини протиправної діяльності, а саме протиправних діянь щодо комерційної, банківської та різних видів професійної таємниці, а так само діянь щодо таємниці волевиявлення. З огляду на поняття комерційної таємниці, що наводиться у ст. 505 Цивільного кодексу України, та банківської таємниці, про яку йдеться у ст. 60 Закону України "Про банки і банківську діяльність", до запропонованого розділу необхідно віднести склади злочинів, передбачені статтями 231 (Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю), 232 (Розголошення комерційної або банківської таємниці), 232¹ (Незаконне використання інсайдерської інформації). Близькою до цієї групи злочинів є й приховування інформації про діяльність емітента (ст. 232²).

Що стосується професійної таємниці, під якою розуміється інформація з обмеженим доступом, яка стала відомою або доступною представнику певної професії у зв'язку з виконанням професійних або поряд з ними службових чи процесуальних обов'язків, незаконне розголошення або використання якої завдає шкоди інформаційній безпеці особи, суспільства чи держави [13, с. 6], то до цього розділу доцільно перемістити такі склади злочинів, що передбачені статтями 132 (Розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби), 145 (Незаконне розголошення лікарської таємниці), 168 (у частині розголошення таємниці усиновлення (удочеріння) службовою особою або працівником медичного закладу, яким відомості про усиновлення (удочеріння) стали відомі по службі чи по роботі), 209¹ (Умисне порушення вимог законодавства про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансування тероризму (у частині розголошення інформації з питань фінансового моніторингу особою, якій ця інформація стала відома у зв'язку з професійною або службовою діяльністю), 330 (Передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни), 381 (Розголошення відомостей про заходи безпеки щодо особи, взятої під захист), 387 (Розголошення даних оперативно-розшукової діяльності, досудового розслідування). У свою чергу, порушення таємниці волевиявлення особи може полягати у здійсненні дій, передбачених ст. 159 (Порушення таємниці голосування).

По-третє, логічним так само уявляється включення до розділу “Злочини проти інформаційної безпеки особи, суспільства, держави” складів злочинів, пов'язаних із порушенням державної таємниці, а саме: статті 328 (Розголошення державної таємниці), 329 (Втрата документів, що містять державну таємницю), 422 (Розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості). Об'єктом перелічених злочинів виступають суспільні відносини з охорони державної таємниці в різних сферах діяльності держави, що можна охарактеризувати як відносини інформаційної безпеки [8, с. 689].

По-четверте, злочинами, що фактично порушують право особи на власну інформаційну безпеку приватного життя, положення про яку чітко сформульовані у статтях 31 і 32 Конституції України, слід вважати порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163) та порушення недоторканності приватного життя (ст. 182). Отже, ці склади кримінально караних правопорушень так само доцільно перемістити до єдиного розділу КК України, про який йдеться.

По-п'яте, вважати злочинами, що, у тому числі, порушують порядок циркуляції певної інформації й у такий спосіб посягають на упорядкованість інформаційного простору, пов'язаного з належною реалізацією та правовим забезпеченням авторського права й права на інтелектуальну власність, доцільно й діяння, передбачені статтями 176 (Порушення авторського права і суміжних прав) і 177 (Порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію).

По-шосте, велику шкоду суспільним відносинам у сфері інформаційного простору завдають злочини, пов'язані з пропагандою, у тому числі в засобах масової інформації, культу насильства і жорстокості, расової, національної чи релігійної нетерпимості та дискримінації (ст. 300), а так само з поширенням порнографії (ст. 301). Наприклад, лише у 2019 р. за ст. 301 КК в Україні було зареєстровано 1012 злочинів. Ці діяння, посягаючи

на засади суспільної моральності в сфері духовного й культурного життя, безумовно, зачіпають і безпеку сфери інформаційного простору, завдаючи учасникам (суб'єктам) цієї сфери неабиякої шкоди. Включення цієї групи злочинів до єдиного розділу під назвою “Злочини проти інформаційної безпеки особи, суспільства, держави”, напевно, викликати чимало заперечень. Однак як робочу гіпотезу варіант з їх віднесенням до знов створеного розділу, на нашу думку, не слід беззаперечно відкидати.

По-сьоме, у порядку *de lege ferenda* до єдиного Розділу “Злочини проти інформаційної безпеки особи, суспільства, держави” слід внести злочин або злочини, пов’язані з поширенням дезінформації (звісно ж, якщо буде прийнятий Закон України “Про протидію дезінформації”).

Що стосується техніки об’єднання перелічених кримінально караних правопорушень в єдиному розділі Кодексу, то це можна зробити шляхом виключення відповідних статей із тих розділів, в яких вони знаходяться зараз, та присвоєння їм нової нумерації в тому “базовому” розділі, до якого планується їх перенести. У майбутньому ж Кримінальному кодексі, робота над яким активно триває у цей час, висловлена пропозиція у технічному плані не викликати жодних перешкод, оскільки всім статтям буде присвоєна нова нумерація. Єдине, на що треба звернути у майбутньому увагу: чи будуть ті або інші правопорушення віднесені до злочинів або до кримінальних проступків. Від цього залежатиме їх знаходження чи то в Кримінальному кодексі України, чи то у Кодексі про кримінальні правопорушення України.

Інформаційна безпека особи, суспільства та держави так само може потерпати ще від цілої низки злочинів. Йдеться принаймні про злочини, передбачені статтями 109 (Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади), 110 (Посягання на територіальну цілісність і недоторканність України), 111 (Державна зрада) та 114 (Шпигунство) КК України. На теперішній час перелічені злочини охоплюються розділом I Особливої частини КК України, що має назву “Злочини проти основ національної безпеки України”. На наш погляд, ці склади злочинів потребують особливого виокремлення в самостійному розділі законодавства про кримінальну відповідальність, адже вони посягають на ті, так би мовити, фундаментальні суспільні відносини, що забезпечують існування й розвиток України як суверенної, незалежної, демократичної, соціальної й правової держави на сучасній політичній карті світу.

Висновки.

Теоретичне дослідження питань захисту інформаційного простору Української держави дозволяє стверджувати, що особливістю нинішньої моделі захисту інформаційних відносин засобами кримінального права є те, що відповідні норми містяться в різних розділах Особливої частини КК України. Принаймні можна виділити сім блоків правопорушень (з урахуванням злочинів проти основ національної безпеки України), що так чи інакше безпосередньо можуть завдавати шкоду цій сфері життєдіяльності суспільства. У цьому вбачається деяка штучність законодавчого підходу до захисту єдиного інформаційного простору та виникнення джерела нескінченної дискусії про первинність захисту відповідними нормами чи то кіберпростору, чи то простору, яким, окрім кіберпростору, охоплюються ще й інші площини інформаційного комунікування різноманітних суб'єктів (соціальних інституцій та їх представників, окремих осіб, великих колективів або навіть народів).

Ефективна модель захисту інформаційних відносин, що існують у суспільстві, засобами кримінального права, передбачає насамперед акумуляцію норм, що

здійснюють захист всіх суб'єктів, яким може завдаватися шкода (особа, суспільство та держава) переважною більшістю відповідних злочинів, в єдиному розділі КК України.

Водночас має йтися не про захист інформаційних відносин у вузькому їх розумінні, а про захист саме інформаційного простору як специфічного середовища, яке пов'язане з протіканням різноманітних інформаційних процесів із приводу створення, обігу інформації та захисту як самої інформації у будь-якій з її форм, інформаційних продуктів і послуг, так й інструментів її циркуляції у суспільстві. Такий хід міркувань зумовлює створення об'єднаної "платформи" захисту відповідних суспільних відносин у вигляді єдиного розділу Особливої частини КК України.

Використана література

1. Тарасюк А.В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. № 4(31)/2019. С. 73-82.
2. Писаренко Г.М. Юридична відповідальність в інформаційній сфері: окремі аспекти становлення. *Науковий вісник Ужгородського національного університету. Серія ПРАВО*. 2016. Вип. 36. Т. 2. С. 55-58.
3. Про основи національної безпеки України: Закон України від 19.06.03 р. № 964-IV. *Відомості Верховної Ради України*. 2003. № 39. Ст. 351.
4. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
5. Стратегія національної безпеки України: Указ Президента України від 26.05.15 р. № 287/2015. *Офіційний вісник Президента України*. 2015 р. № 13. Ст. 874.
6. Міністр культури презентував законопроект про протидію дезінформації. URL: <https://www.sud.ua/ru/news/publication/159088-ministr-kulturi-prezentuvav-zakonoprojekt-pro-protid-iyu-dezinformatsiyi> (дата звернення 18.02.2020).
7. Попова Т.В., Ліпкан В.А. Стратегічні комунікації (словник); за ред. В.А. Ліпкана. Київ: ФОПС. Ліпкан, 2016. 416 с.
8. Кримінальний кодекс України: науково-практичний коментар. Особлива частина. У 2 т. Т. 2. 5-те вид., доп.; за ред. В.Я. Тація, В.П. Пшонки, В.І. Борисова, В.І. Тютюгіна. Ю.В. Баулін. Харків: Право, 2013. 1040 с.
9. Про кіберзлочинність: Конвенція Ради Європи від 23 листопада 2001 року. ETS № 185. *Офіційний вісник України*. 2007. № 65. Ст. 2535.
10. Юрченко А.В., Дудченко А.Д. Security Management for Business. Тема № 10 (2015).pdf. – (Презентація). URL: <http://www.myshared.ru/slide/980543> (дата звернення 22.02.2020).
11. Про протидію дезінформації. – (Презентація законопроекту). URL: <https://www.mkms.gov.ua/files/InformPolityka.pdf> (дата звернення 18.02.2020).
12. Пояснювальна записка до проекту Закону України "Про внесення змін до деяких законодавчих актів України щодо відповідальності за посягання у сфері інформаційної безпеки". URL: http://www.search.ligazakon.ua/l_doc2.nsf/link1/GF7DZ00A.html (дата звернення 06.02.2020).
13. Резнікова Г.І. Криміналістична характеристика злочинів щодо розголошення професійних таємниць: автореф. дис. ...канд. юрид. наук: 12.00.09. – (Нац. юрид. ун-т імені Ярослава Мудрого). Харків, 2015. 20 с.

~~~~~ \* \* \* ~~~~~

**Інформація за іншими предметними напрямками досліджень за спеціалізаціями в галузі знань 08 – “Право”**

УДК 346.544.4:004

**ЖОРНЯК А.В.**, аспірантка кафедри господарського права  
Національного юридичного університету ім. Ярослава Мудрого.

**ПРО ПІДХОДИ ДО КЛАСИФІКАЦІЇ ІНФОРМАЦІЙНИХ ПОСЛУГ  
У СФЕРІ ГОСПОДАРЮВАННЯ**

**Анотація.** В останні роки в Україні спостерігається тенденція до збільшення частки ринку інформаційних послуг в економіці країни. Це пов'язано не тільки зі збільшенням об'єму наданих інформаційних послуг (кількісний показник), але й з появою нових видів таких послуг (якісний показник). Розвиток інформаційного суспільства, впровадження інформаційних технологій в усі сфери діяльності суб'єктів господарювання вимагає від законодавця адекватного правового регулювання окреслених відносин з метою ефективного захисту прав та інтересів кожного учасника ринку інформаційних послуг. Зважаючи на зазначене, логічно-структурне впорядкування (класифікація) інформаційних відносин має важливе значення в процесі їх законодавчої та доктринальної регламентації. Автором проаналізовано наявні у правовій науці підходи до диференціації інформаційних послуг та запропонована власна класифікація окресленої сфери послуг.

**Ключові слова:** види інформаційних послуг, класифікація, господарські відносини, інформація, суб'єкт господарювання, детермінуюча ознака.

**Summary.** In recent years, there has been a tendency in Ukraine to increase the market share of information services in the country's economy. This is due not only to the increase in the volume of information services provided (quantitative indicator), but also to the emergence of new types of such services (qualitative indicator). The rapid development of the information society, the introduction of information technology in all spheres of activity of business entities requires the legislator to adequately regulate the outlined relations in order to effectively protect the rights and interests of each participant in the information services market. In view of the above, logical and structural organization (classification) of information relations is important in the process of their legislative and doctrinal regulation. The author analyzes the approaches to the differentiation of information services available in legal science and proposes her own classification of the defined sphere of services.

**Keywords:** types of information services, classification, economic relations, information, entity, determinant.

**Аннотация.** В последние годы в Украине наблюдается тенденция к увеличению доли рынка информационных услуг в экономике страны. Это связано не только с увеличением объема предоставляемых информационных услуг (количественный показатель), но и с появлением новых видов таких услуг (качественный показатель). Развитие информационного общества, внедрение информационных технологий во все сферы деятельности субъектов хозяйствования требует от законодателя адекватного правового регулирования указанных отношений с целью эффективной защиты прав и интересов каждого участника рынка информационных услуг. Таким образом, логически-структурное упорядочение (классификация) информационных отношений в части предоставления услуг имеет важное значение в процессе их законодательного и доктринального регулирования. Автором проанализированы имеющиеся в правовой науке подходы к дифференциации информационных услуг, а так же предложена собственная классификация данной сферы услуг.

**Ключевые слова:** виды информационных услуг, классификация, хозяйственные отношения, информация, субъект хозяйствования, детерминирующий признак.

**Постановка проблеми.** На сьогодні в законодавстві України та правовій науці не існує єдиної класифікації інформаційних послуг, яка б могла структурувати суспільні відносини в цій сфері, а також регламентувати діяльність суб'єктів господарювання в межах окресленої проблематики. Справедливо зазначити, що відносини у сфері надання інформаційних послуг є багатогранними та динамічними, що обумовлює існування багатьох критеріїв та ознак для класифікації. Крім цього, на доктринальному рівні спостерігається множинність підходів до зазначеного питання, на підставі чого виникає потреба в їх аналітичному осмисленні та узагальненні. Зростання актуальності вказаної теми обумовило підвищення інтересу до вивчення інформаційних послуг у різних галузях науки.

**Результати аналізу наукових публікацій.** Окремі види інформаційних послуг досліджувалися такими вченими-юристами, як Ю.П. Бурило [1], В.С. Мілаш [2], Р.В. Ваксман [3], В.М. Брижко [4], А.С. Пешковою [5], Л.В. Санніковою [6], Л.Б. Ситдиковою [7], В.М. Когут [8]. Значний вклад у вирішення питання класифікації інформаційних послуг здійснили вчені-економісти С.Ю. Демін [9], С.Д. Подпругін, В.Л. Тамбовцев [10]. Водночас в юридичній науці на сьогодні не вироблено єдиного підходу до класифікації інформаційних послуг, не достатньо вивчені їх окремі види, що загалом негативно впливає й суттєво віддаляє створення законодавцем ефективного механізму правового регулювання відносин у сфері надання інформаційних послуг.

**Метою статті** є оцінка аналізу відносин, які виникають у процесі надання інформаційних послуг, їх упорядкування та логічне структурування (класифікація) для створення належних умов щодо здійснення подальшого теоретичного дослідження та правового регулювання.

**Виклад основних положень.** В умовах стрімкого поширення глобалізаційних процесів одним із пріоритетних напрямків для України є розвиток інформаційного суспільства, цифровізація економіки та впровадження інформаційно-комунікаційних технологій в усі сфери життєдіяльності населення, суб'єктів господарювання, особи та держави.

Досвід багатьох держав свідчить, що інформаційні технології стали рушійною силою в розвитку соціально-економічного сектору, прискорили перехід до постіндустріального типу економіки, а також розширили сферу послуг та нематеріального виробництва економічних благ.

На сьогодні інформаційні послуги, як важливий елемент інформаційної економіки та сектор ринку послуг, що постійно зростає, потребують адекватного правового регулювання та системного упорядкування. Одним із способів організації такої складної системи суспільних відносин є класифікація, під якою розуміють підпорядкованість понять певній ознаці та встановлення взаємозв'язків між ними.

Дослідження питання видів інформаційних послуг у сфері господарювання доречно розпочати з аналізу чинної статистичної класифікації видів економічної діяльності в окреслених правовідносинах.

У Наказі Держспоживстандарту від 11.10.10 р. № 457, яким затверджено Національний класифікатор України, зокрема у розділі “Інформація та телекомунікації”, серед інших виокремлюється такий вид економічної діяльності як надання інформаційних послуг, з диференціацією на підвиди, а саме: оброблення даних, розміщення інформації на вебвузлах і пов'язана з ними діяльність, веб-портали, діяльність інформаційних агентств, надання інших інформаційних послуг [11].

Оскільки інформаційна послуга як теоретико-правова категорія є поняттям більш широким, вона може охоплювати наступні види економічної діяльності: діяльність у

сфері права, діяльність у сфері бухгалтерського обліку й аудиту; консультування з питань оподаткування, консультування з питань керування, рекламна діяльність і дослідження кон'юнктури ринку, надання послуг перекладу, діяльність туристичних агентств, туристичних операторів, надання інших послуг із бронювання та пов'язана з цим діяльність, освіта, охорона здоров'я. Характер діяльності суб'єктів господарювання в окреслених сферах, як правило, полягає у створенні, обробці та наданні певного обсягу інформації замовнику, а тому може розглядатися як різновид інформаційних послуг.

Така легальна статистична диференціація, на жаль, не в повному обсязі окреслює інформаційні послуги, як окремий вид інформаційної економічної діяльності, який, фактично, вже встиг сформуватися, а тому не відповідає потребам сучасного ринку інформаційних послуг і надалі потребує розширення та удосконалення.

Як зазначає В.С. Мілаш, видоутворювальною ознакою інформаційних послуг є сама інформація, яка одночасно є і об'єктом впливу виконавця послуг, дії якого спрямовані на зміну її стану, і результатом їх надання, який отримує матеріальне втілення у планах, звітах, пропозиціях тощо [2, с. 72].

Дійсно, в умовах активного виробництва та використання інформаційних продуктів у процесі господарської діяльності, інформація набуває домінуючого та визначального значення. Тому необхідним є врахування її правової природи та юридичних властивостей які можуть впливати на регулювання окреслених відносин. У цьому контексті цікавим питанням є правовий режим інформації, як об'єкта відносин у сфері надання інформаційних послуг. Так А. Дідук зазначає, що “під правовим режимом інформації, конфіденційної інформації (комерційної таємниці та ноу-хау) слід розуміти “врахування” законодавцем природних властивостей та ознак, які їм притаманні” [12]. Насправді ж у законодавстві України вказаного терміна не існує, а Закон України “Про інформацію” оперує поняттям “режим доступу” на підставі якого виділяє відкриту інформацію та інформацію з обмеженим доступом, де остання в господарському обігу виступає як конфіденційна інформація (комерційна таємниця) [13].

Особливість режиму доступу до вказаної конфіденційної інформації полягає в її комерційній цінності, не загальновідомості, обмеженні доступу до неї третіх осіб, що тягне за собою певні правові наслідки та обумовлює різні правові режими інформації.

З огляду на викладене, на нашу думку, інформаційні послуги можна розрізняти в залежності від режиму доступу до інформації, яка становить інформаційний продукт у конкретних відносинах, а саме: *інформаційні послуги, які містять лише відкриту інформацію та інформаційні послуги, які містять у собі інформацію з обмеженим доступом.*

Важко не погодитись з вченими, які визначають інформаційну послугу, як об'єкт та інституційний елемент інформаційного ринку. Зважаючи на те, що в економічній науці існують розробки з поділу інформаційного ринку на сектори, логічно припустити, що така обставина може виступити детермінуючою ознакою при класифікації інформаційних послуг.

Так В.Л. Тамбовцев запропонував п'ять макросекторів інформаційного ринку:

- науково-технічна продукція; об'єднує проектні розробки з подальшим розподілом у галузевому розрізі, технологічні, у тому числі методичного характеру, з аналогічним розподілом, власне наукові розробки, що слугують своєрідним “напівфабрикатом” для попередніх груп інформаційних продуктів, з аналогічним галузевим розподілом;

- об'єкти художньої культури; до них належать текстова (книжково-журнальна), візуальна (кіно, відео, театральнo-видовищна, живописна) та аудіопродукція;

- управлінські дані й повідомлення; у даний сектор включено: політичну й господарську інформацію, статистичні дані, дані про ринкову ситуацію, рекламні повідомлення, оцінки і рекомендації прийняття рішень (ділові консультації);

- побутова інформація; об'єднує повідомлення загальноорієнтаційного характеру, відомості про споживчий ринок і відомості про ринок праці;

- послуги освіти; включають дошкільне, шкільне, позашкільне, післяшкільне, середнє спеціальне і післявузівське (перепідготовка і підвищення кваліфікації) навчання [10].

На підставі вищенаведеного, на нашу думку, доцільно розрізняти інформаційні послуги в залежності від сектору інформаційного ринку, в межах якого вони надаються.

Крім цього, на сьогодні, на теоретичному рівні існують різні підходи щодо віднесення тих чи інших видів діяльності, пов'язаних з інформацією, до інформаційних послуг, особливо це стосується передачі (транслявання) інформації. Так, на думку Л. Ситдикової, послуги зв'язку не можна відносити до інформаційних послуг, так як відсутня її функціональна ознака – інформаційний запит, а послуги зв'язку є лише засобом передачі інформації [7, с. 42].

Дослідник Ю.П. Бурило за об'єктом впливу виділяє інформаційні та інформаційно-інфраструктурні послуги. Якщо для інформаційних робіт і послуг таким об'єктом є змістовна інформація – “контент”, то для інформаційно-інфраструктурних – елементи інформаційно-телекомунікаційної інфраструктури. У зв'язку з цим відрізняються між собою інформаційні і телекомунікаційні послуги. Тоді як інформаційні послуги, як правило, передбачають надання споживачеві певного контенту, телекомунікаційні послуги як різновид інформаційно-інфраструктурних послуг насамперед забезпечують доступ до телекомунікаційної мережі (інформаційно-телекомунікаційної інфраструктури) [1, с. 38].

На думку Пешкової А.С., при забезпеченні телефонного зв'язку оператор не надає власне інформаційних послуг, оскільки при цьому він не надає інформацію [5, с. 57].

Отже, як бачимо, *не всі послуги, які належать до інформаційної сфери є інформаційними*. На нашу думку, детермінуючою ознакою в даному випадку слід вважати інформацію (інформаційний продукт), яка постає безпосереднім об'єктом впливу в процесі надання інформаційної послуги. Враховуючи стрімкий розвиток інформаційних технологій, а також з метою уникнення підміни понять, було б доречно, поряд з інформаційними послугами, виокремити *послуги, що надаються у межах інформаційної сфери*. До останніх можна віднести широке коло послуг у сфері зв'язку, телекомунікацій, послуг доступу до мережі Інтернет, хостингу, поштового зв'язку та інші. Такі послуги безпосередньо не стосуються інформаційного продукту, мають “обслуговуючий” характер та є допоміжними і часто передують самим інформаційним послугам. Так, наприклад, самі по собі провайдерські послуги, які полягають у наданні доступу споживачам до мережі Інтернет, не пов'язані з інформаційними продуктами, однак вони створюють необхідну передумову для отримання електронних інформаційних послуг.

Інформаційна послуга, як правило, становить собою послідовний процес із забезпечення споживачів інформаційними продуктами, який вимагає від виконавця вчинення ряду пов'язаних між собою дій. Так, наприклад, О. Тур визначає консультаційну послугу, як інтелектуальну діяльність неуречевленого характеру, яка здійснена професійним консультантом на оплатній чи безоплатній основі, в процесі якої консультант надає замовнику інформацію у вигляді порад, рекомендацій, висновків із питань, визначених замовником у різноманітних сферах діяльності в матеріалізований

формі, доступній для об'єктивного сприйняття [14, с. 16]. Із зазначеного випливає, що консультаційна послуга, як різновид інформаційної, може передбачати спочатку пошук, збір, аналіз, обробку, і як результат цього процесу – передачу інформаційного продукту споживачеві в зрозумілій для нього формі.

Інформаційно-аналітична правова система “Ліга:Закон” також передбачає надання інформаційних послуг шляхом відкриття доступу до свого інформаційного ресурсу, у межах якого споживачі самі здійснюють пошук інформації в залежності від їхніх інформаційних потреб.

Ще більш різноманітними з точки зору інформаційних процесів є інформаційні послуги у сфері рекламної діяльності. Так, на думку Т. Партин, рекламна діяльність – діяльність суб'єктів господарювання, пов'язана з визначенням потреби створення й розміщення реклами задля досягнення стратегічних і поточних завдань їхнього розвитку. Рекламна діяльність охоплює сукупність процесів дослідження ринку збуту й визначення потреби в рекламі, дослідження ринку рекламних засобів та рекламної аудиторії, формування стратегії та програми рекламної діяльності, створення рекламного продукту, його публікації чи показу в засобах масової інформації, дослідження ефективності здійснення рекламних акцій та рекламної діяльності загалом [15].

Б. Обритько вважає, що рекламна діяльність є комплексом організаційних і технічних рекламних заходів, спрямованих на створення і підтримку необхідного рівня продажу продукції, швидке реагування на зміну ринкової кон'юнктури, прийняття необхідних заходів для нейтралізації діяльності конкурентів, забезпечення позитивного іміджу фірми і її торгової марки [16, с. 12-13].

На думку Р. Ваксман, “рекламна діяльність є невід'ємною складовою функціонування будь-якого товарного ринку, самостійним видом комерційної господарської діяльності (підприємницької), яка здійснюється на конкурентних засадах та полягає у проектуванні, виготовленні та розміщенні замовленого або наданого контрагентом рекламного продукту й розповсюдженні з метою впливу на реципієнтів-споживачів задля активізації збуту відповідних товарів та послуг, а також інформування їх щодо суспільно значущих фактів та подій” [3, с. 18].

Як бачимо, інформаційні послуги становлять собою множинність процесів, що ускладнює класифікацію інформаційних послуг за функціональною ознакою, і, відповідно, виокремлення конкретної детермінуючої дії інформаційного процесу.

З цього приводу можна погодитися з думкою Л.В. Саннікової про те, що така дія, як передача інформації споживачеві є завершальним етапом інформаційної послуги [6, с. 102]. Тобто їй передують одна або декілька дій, спрямованих на забезпечення споживача необхідною інформацією, а сама по собі передача інформаційного продукту споживачеві не є видоутворювальною ознакою. Таким чином, *за характером ключової дії*, що здійснює виконавець, доречно виокремити інформаційні послуги: зі збору (включає пошук та передачу), обробки та аналізу (інформація надається самим споживачем, однак потребує опрацювання та передачі виконавцем), надання доступу (споживач отримує можливість самостійно здійснювати пошук у відповідних інформаційних базах, платформах і т.д.). Такий поділ є досить умовним, оскільки будь-яка інформаційна послуга включає в себе декілька процесів, що взаємопов'язані між собою.

Вартими уваги є дослідження у цій сфері економістів С.Ю. Деміна та С.Д. Подпругіна. Науковці класифікують інформаційні послуги за видами потреб, що задовольняються, на наступні: послуги зі збору інформації (консалтингові послуги),

послуги з пошуку інформації (пошукові системи в мережі Інтернет), послуги з передачі інформації (телекомунікаційні мережі) послуги з обробки інформації (проектні послуги), послуги зі зберігання інформації (запис інформації на різних носіях, у тому числі оптичних), послуги з надання інформації (послуги віддалених баз даних), послуги з поширення інформації (рекламна діяльність).

Крім цього, дослідники диференціюють інформаційні послуги за формою їх надання і виділяють: інформаційні послуги, які потребують участі споживача та інформаційні послуги, які не потребують участі споживача. [9, с. 54] Проте учені не уточнюють форми та змісту такої участі споживача в інформаційній послугі. Звідси виникає питання чи може інформаційний запит споживача вважатися участю в наданні послуги? Чи передбачає така участь вчинення певних дій з боку споживача в процесі надання йому інформаційної послуги? На нашу думку, вказана класифікація є спірною, оскільки будь-яка інформаційна послуга здійснюється за запитом і з метою задоволення інформаційних потреб споживача, що тягне за собою необхідність його безпосередньої участі хоча б на початковому етапі. Тобто, фактично, споживач виступає ініціатором та обов'язковим учасником процесу надання будь-якої інформаційної послуги.

Окремої уваги, на нашу думку, заслуговує диференціація інформаційних послуг *залежно від засобів комунікації*, що використовуються в процесі їх надання споживачу. Так у контексті вказаної ознаки можна виділити інформаційні послуги які надаються за допомогою телефонного, поштового, факсового зв'язку, особистого звернення, електронних мереж.

Розвиток інформаційних технологій надав можливість обміну інформацією між суб'єктами у віртуальному просторі в режимі он-лайн. Зважаючи на стрімку "діджиталізацію" всіх галузей суспільного виробництва, поділ інформаційних послуг залежно від способу їх надання є цілком виправданим. Більше того, впродовж останніх років у законодавстві та науці все частіше зустрічається поняття електронної інформаційної послуги.

Так В.М. Когут визначає електронну послугу як будь-яку надану інформаційну або іншу послугу, яка виникає в процесі інформаційної діяльності за допомогою інформаційно-комунікаційних технологій та охоплює усі сфери діяльності, а також є одним з результатів діяльності державних службовців і обов'язково пов'язана з системою електронного уряду. [8]

Закон України "Про електронну комерцію" від 03.09.15 р. визначає інформаційні електронні послуги як платні або безоплатні послуги щодо оброблення та зберігання інформації, що надаються дистанційно з використанням інформаційно-телекомунікаційних систем за індивідуальним запитом їх одержувача [17].

Зазначене дає нам підставу для виділення за способом передачі інформації підвиду інформаційних послуг, а саме: інформаційних *електронних послуг*, які надаються із залученням засобів інформаційних технологій, наприклад, за допомогою мережі Інтернет або інших інформаційно-телекомунікаційних інструментів.

У дослідженні відносин в сфері інформаційних послуг, окремої уваги заслуговує "Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд", затверджений Наказом Державного комітету зв'язку та інформатизації України від 15.08.03 р. № 149, який визначає процедуру надання органами виконавчої влади інформаційних та інших послуг громадянам і юридичним особам з використанням електронної інформаційної системи "Електронний Уряд". Зокрема, розрізняються чотири види електронного надання інформаційної послуги:

- інформування (надання безпосередньо інформації про державні (адміністративні) послуги);
- одностороння взаємодія (забезпечена можливість користувачу отримати електронну форму документа);
- двостороння взаємодія (забезпечена можливість обробки електронної форми документа, включаючи ідентифікацію);
- проведення трансакцій (електронна реалізація можливостей прийняття рішень та їх доставка).

Наразі Кабінет Міністрів України надає громадянам та бізнесу 119 електронних послуг. Серед тих послуг, які вже доступні он-лайн, є:

- послуги у соціальній сфері: оформлення допомоги при народженні дитини, житлової субсидії, низка послуг Пенсійного фонду України;
- послуги для бізнесу: реєстрація бізнесу, оформлення ліцензій та дозволів, отримання виписок і довідок он-лайн;
- послуги у будівельній сфері, завдяки чому вже 80 % будівництва в Україні можна починати та вводити в експлуатацію он-лайн (стосується класу СС1). У цій сфері введено першу повністю автоматичну електронну послугу, без жодного контакту з чиновниками – початок будівельних робіт для класу СС1;
- послуги у сфері безпеки та суду, завдяки яким можна он-лайн отримати довідки про несудимість, відсутність корупційних правопорушень, подати заяву до суду;
- послуги для автовласників: зокрема, електронний кабінет водія – зручний онлайн-інструмент, який дозволяє кожному автовласнику отримувати інформацію про свій транспортний засіб, водійські посвідчення, штрафи, записуватися в е-чергу для візитів до сервісних центрів МВС тощо;
- послуги у транспортній сфері: зокрема, електронний кабінет перевізника, який дозволяє автоперевізникам оформити, розширити, звузити, анулювати ліцензії на перевезення пасажирів та вантажів, а також – зручно та оперативно вносити зміни до відомостей про свої підприємства [18].

Наведені різновиди інформаційних послуг надаються у процесі позадоговірних відносин та у межах адміністративних повноважень органів державної влади та місцевого самоврядування.

У зв'язку зі стрімким поширенням використання інформаційних технологій як одного із основних засобів комунікації між суб'єктами, відбувається прямо пропорційне збільшення обсягів і кількості електронних інформаційних послуг, серед яких виникають якісно нові послуги, а також вже наявні інформаційні послуги трансформуються в електронні інформаційні послуги. Звідси, на нашу думку, виникає підміна двох різних понять, які несуть у собі різне значення. Так серед електронних інформаційних послуг необхідно вирізнити ті, які за своєю природою можуть надаватися *лише із використанням засобів телекомунікаційного зв'язку, а значення "електронні" є їх якісною характеристикою, поза межами якої вони існувати не можуть, наприклад* телемедицина, послуги з програмування, створення вебсайту, SMM – маркетинг у соціальних мережах і т.д.

Іншу групу інформаційних електронних послуг становлять ті послуги, у процесі надання яких електронний зв'язок використовується як один із способів передачі інформації, з метою швидкості, зручності, виключення корупційного чинника, економії матеріальних ресурсів і т.д. Такі інформаційні послуги надаються в умовах безпосередньої комунікації суб'єктів без використання телекомунікаційних технологій, однак у зв'язку зі стрімким поширенням і здатністю спрощення певних процесів

останніх, трансформуються в електронні інформаційні послуги. У цьому випадку така характеристика як “електронні” інформаційні послуги вказує на спосіб передачі інформації.

На сьогоднішній день особливої актуальності у рамках договірних господарсько-виробничих відносин набирають послуги електронного банкінгу, електронного маркетингу, дистанційні освітні послуги, послуги зі створення вебсайту і т.д., тому вказана диференціація інформаційних послуг у сучасних умовах є необхідною та виправданою.

Зважаючи на те, що предметом дослідження цієї статті є класифікація інформаційних послуг у сфері господарювання, це потребує врахування особливостей господарських правовідносин. Йдеться, зокрема, про специфічний суб’єктний склад, який чітко окреслений у законодавстві.

Так у Господарському кодексі України зазначається, що учасниками відносин у сфері господарювання, серед інших, є суб’єкти господарювання. Договірна форма інформаційних послуг у сфері господарювання може виникати лише в межах господарсько-виробничих відносин, тобто таких, що виникають між суб’єктами господарювання при безпосередньому здійсненні господарської діяльності. З цього випливає, що лише суб’єкти господарювання можуть виступати сторонами в процесі надання інформаційних послуг в окресленій галузі правовідносин.

Слід зазначити, що питанню суб’єктного складу відносин у сфері надання інформаційних послуг у правовій науці приділялося замало уваги. Більшість вчених, спираючись на загальні положення про надання послуг, традиційно виділяють двох суб’єктів: замовник (споживач) з одного боку, та виконавець (послугонадавач) – з іншого. Однак, аналізуючи сучасний ринок інформаційних послуг, можна стверджувати про наявність ще одного суб’єкта окреслених відносин – інформаційного посередника. Особливої актуальності набуло це питання у сфері електронної комерції, оскільки на сьогодні національні ринки послуг вже не можуть функціонувати повноцінно без залучення інструментів електронної комунікації (Інтернет-технології, електронні платіжні системи, електронний документообіг).

Так В.В. Рєзнікова відносить комерційних посередників до інфраструктури товарного ринку і визначає зміст їх діяльності як здійснення будь-яких правомірних дій юридичного та/або фактичного характеру в інтересах та за рахунок іншого суб’єкта господарювання (замовника) [19, с. 298].

Необхідність інформаційного посередництва викликана, з одного боку, потребою ефективної реалізації послуг на ринку товарів. Так посередник, використовуючи свої професійні зв’язки, ділову репутацію, досвід може більш економічно вигідно для виробника послуг здійснити їх збут, аніж він здійснював це самостійно. З іншого боку, цифровізація ринку послуг та поширення електронної комерції обумовлює інформаційне посередництво для створення фактичних умов надання інформаційних послуг.

Зокрема, А.В. Чучковська метою інформаційного посередництва у сфері електронної комерції визначає забезпечення процесу обміну електронними документами, зберігання їх чи надання інших послуги щодо цих документів [20, с. 10].

Таким чином, у структурі ринку інформаційних послуг серед суб’єктів можемо виділити інформаційного посередника, як одну зі сторін окреслених відносин, що сприяє створенню передумов та ефективному збуту послуг.

Вищезазначене дає нам право виокремити вид інформаційних послуг у сфері господарювання *в залежності від суб’єктного складу* – інформаційна послуга за участю

інформаційного посередника (посередників) та без такої участі. Вказана класифікація дозволяє розширити та деталізувати правовий статус суб'єктів відносин у сфері надання інформаційних послуг, а також удосконалити їх правове регулювання.

### Висновки.

Аналіз господарського законодавства України та наявних наукових підходів до окресленої проблематики дозволив виокремити інформаційні послуги, з-поміж послуг у сфері інформаційних відносин, а також класифікувати їх за режимом доступу до інформації, суб'єктним складом та характером ключової дії виконавця, що дозволить забезпечити якісний механізм правового регулювання договірних відносин у сфері надання інформаційних послуг, з урахуванням їх особливостей.

Подальші наукові дослідження з окресленої тематики передбачають детальне дослідження правового статусу суб'єктного складу та окремих видів інформаційних послуг у сфері господарювання.

### Використана література

1. Бурило Ю.П. Види господарських інформаційних відносин. *Інформація і право*. № 1(7)/2013. С. 35-44.
2. Мілаш В.С. Правові аспекти моделювання договірних відносин, пов'язаних із проведенням маркетингових досліджень. *Вісник господарського судочинства*. 2013. № 1. С. 72.
3. Ваксман Р.В. Проблеми господарсько-правового забезпечення надання рекламних послуг. *Форум права*. 2015. № 3. С. 16-20.
4. Брижко В.М. Інформаційний продукт як об'єкт права власності. *Інформація і право*. № 4(23)/2017. С. 5-15.
5. Пешкова А.С. До визначення поняття телекомунікаційної послуги. *Юридична Україна*. 2008. № 9. С. 54-58.
6. Санникова Л.В. Услуги в гражданском праве России: монография. Москва: Издательство Волтерс Клувер, 2006. 160 с.
7. Сидтикова Л.Б. Современное состояние и нормативно-правовое регулирование отношений в сфере оказания информационных услуг. *Научно-практическое и информационное издание "Гражданское право"*. 2009. № 3. С. 42-51.
8. Когут В.М. Про використання електронних засобів інформації у вітчизняному та зарубіжному законодавстві. URL: <https://www.science.lpnu.ua/sites/default/files/journalpaper/2017/may/2466/vnulpurn201581311.pdf> (дата звернення 17.02.2020).
9. Демин С.Ю., Подпругин С.Д. Рынок информационных продуктов и услуг: сущность, эволюция, специфика. Иркутск, 2007. 176 с.
10. Тамбовцев В.Л. Пятый рынок: экономические проблемы производства информации. Москва: Издательство МГУ, 1993. 127 с.
11. Національний класифікатор України. Класифікація видів економічної діяльності 009:2010: Наказ Держспоживстандарту від 11.10.10 р. № 457. URL: <https://www.zakon.rada.gov.ua/rada/show/ru/vb457609-10/sp:side:max25> (дата звернення 12.02.2020).
12. Дідук А.Г. Правовий режим інформації, конфіденційної інформації (комерційної таємниці та ноу-хау): проблеми. 2013. URL: <https://www.dspace.uzhnu.edu.ua/jspui/bitstream/lib/16424/1.pdf> (дата звернення 05.02.2020).
13. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. URL: <https://www.zakon.rada.gov.ua/laws/show/2657-12> (дата звернення 14.01.2020).
14. Тур О. Консультаційна послуга як юридична категорія. *Підприємництво, господарство і право*. 2015. № 7. С. 64.
15. Партин Т.І. Рекламна діяльність та її інформаційне забезпечення. URL: <http://www.epa.lp.edu.ua:8080/bitstream/ntb/33907/1/42227-230.pdf> (дата звернення 15.02.2020).
16. Обрытько Б.А. Рекламный менеджмент: конспект лекций. Киев: МАУП, 2000. 180 с.

17. Про електронну комерцію: Закон України від 03.09.15 р. № 675-VIII. URL: <https://www.zakon.rada.gov.ua/laws/show/675-19> (дата звернення 04.02.2020).

18. Порядок надання інформаційних та інших послуг з використанням електронної інформаційної системи “Електронний Уряд”: Наказ Державного комітету зв’язку та інформатизації України від 15.08.03 р. № 149. URL: <https://www.zakon.rada.gov.ua/laws/show/z1065-03> (дата звернення 12.02.2020).

19. Рєзнікова В.В. Правове регулювання посередництва у сфері господарювання (теоретичні аспекти): монографія. Київ: Видавництво Хмельницького університету управління та права, 2010. 706 с.

20. Чучковська А.В. Правове регулювання електронної комерції в Україні: навчальний посібник. Київ: Центр учбової літератури, 2007. 223 с.

~~~~~ \* \* \* ~~~~~

УДК 340:342.7

ГОЛОВКО О.М., кандидат юридичних наук, старший науковий співробітник
НДІ інформатики і права НАПрН України.

ДРУЗЬ В.Д., студентка факультету соціології і права,
НТУУ “КПІ ім. Ігоря Сікорського”.

ПРАВО НА ПРАВОСУДДЯ ТА ПРАВО НА ДОСТУП ДО ІНФОРМАЦІЇ: КОРЕЛЯЦІЯ ТА ВЗАЄМОЗАЛЕЖНІСТЬ

Анотація. У статті розглянуто проблеми щодо права на доступ до інформації при альтернативних методах вирішення спорів. Здійснено теоретико-правовий аналіз особливостей функціонування інституту медіації в зарубіжних країнах. Запропоновано шляхи законодавчого вдосконалення механізму доступу громадян до медіації.

Ключові слова: право на інформацію, альтернативні методи вирішення спорів, медіація, права та обов'язки сторін.

Summary. The article discusses the right to access information in case of alternative dispute resolution. The legal analysis of the peculiarities of the functioning of the mediation institute in foreign countries is carried out. The ways of legislative improvement of the mechanism of citizens' access to mediation are suggested.

Keywords: right to information, alternative dispute resolution, mediation, rights and obligations of the parties.

Аннотация. В статье рассмотрены проблемы права на доступ к информации при альтернативных методах разрешения споров. Проведен правовой анализ особенностей функционирования института медиации в зарубежных странах. Предложены пути законодательного совершенствования механизма доступа граждан к медиации.

Ключевые слова: право на информацию, альтернативные методы разрешения споров, медиация, права и обязанности сторон.

Постановка проблеми. Однією з основних сучасних тенденцій розвитку держави є забезпечення та реалізація прав і інтересів громадян. Наразі, українська судова система є перенавантаженою, що унеможливорює оперативне і швидке вирішення спорів, саме тому виникає необхідність у зверненні до альтернативних методів вирішення спору. Проте необхідно забезпечити законодавче закріплення обов'язку належного повідомлення учасників спору щодо можливості звернення до посередника з роз'ясненням щодо їх прав та процедури врегулювання конфлікту для подальшої реалізації цього механізму сторонами.

Результати аналізу наукових публікацій. Емпіричною базою дослідження є Конституція та закони України, інші нормативно-правові акти, законодавство зарубіжних держав, міжнародні та європейські конвенції. У дослідженні використовуються позиції науковців: Волковицька Н., Карташов М., Катаєва Е. та інших.

Метою статті є забезпечення доступу права на інформацію при альтернативних методах вирішення спорів, шляхом здійснення компаративного аналізу міжнародного та національного законодавства.

Для досягнення вказаної мети ставилися завдання:

- проаналізувати особливості медіації як одного з альтернативних способів урегулювання спору та його співвідношення з правом на доступ до правосуддя;

- дослідити забезпечення права на доступ до інформації при альтернативних методах вирішення спорів;
- виявити проблеми, через які неможливо забезпечити вирішення спору шляхом звернення до медіації.

Виклад основного матеріалу. Принцип верховенства права є однією з невід'ємних складових правової та демократичної держави, а тому реалізація його елементів є одним з пріоритетних векторів правової політики. Відповідно до основного закону України, правове регулювання суспільних відносин здійснюється державою для виконання основного обов'язку – забезпечення громадянам України належних умов для можливості реалізації своїх суб'єктивних прав та юридичних обов'язків.

Одним із шести основних елементів принципу верховенства права закріпленого рішенням Венеціанської комісії є доступ до правосуддя [1], завдяки чому забезпечується можливість у разі порушення, невизнання чи оспорювання права звернення до суду для захисту своїх інтересів. Наразі в Україні активно відбувається впровадження судової реформи, яка покликана вирішити проблеми сучасного судочинства, зокрема розподілення справ та завантаженість судів.

Один з найбільш завантажених судів в Україні – Печерський районний суд міста Києва – розглядає 278 судових справ, враховуючи той факт, що усього в суді працює лише 31 суддя [2], що фактично не може забезпечити право особи на повний і всебічний розгляд справи, через перезавантаженість. Тому суд не має змоги реалізувати право особи на інформацію, зокрема, розширено та деталізовано пояснити усі права і обов'язки сторін.

Якщо ж звернутися до судів касаційних інстанцій, то вони також перевантажені. Відповідно до статистичних даних Верховного Суду України (далі – ВС України), то розпочинаючи з 01.01.2020 до 28.02.2020 роки у ВС України було розглянуто 15307 клопотань, заяв та скарг – 7818 справ [3].

Законом передбачається можливість звернення до Європейського Суду з прав людини (далі – ЄСПЛ), у разі якщо наявні в Україні можливості звернення до національних інстанцій вичерпано, але були порушені основоположні права та інтереси людини або ж принципи здійснення правосуддя. Майже чверть звернень до ЄСПЛ – проти України. Проте для цього необхідно вичерпати звернення до усіх національних інстанцій – перша інстанція, апеляційна та касаційна, що, враховуючи завантаженість національних інстанцій, може займати велику кількість часу, а отже нівелює реалізацію права на справедливий суд, оскільки не може забезпечити оперативність розгляду справи.

Якщо ж звернутися до самого процесу розгляду справи (на прикладі цивільного або господарського процесу), то суд зобов'язується повідомити сторони про право на укладання мирової угоди (ст. 182 ГПК України) [4], завдяки чому можливе швидке досягнення компромісу сторонами. Зокрема, в судовому засіданні суд в особі судді запитує у сторін, щодо бажання укласти мирову угоду. В цьому випадку задовольняються вимоги обох сторін частково, адже мирова угода базується на основі взаємних поступок, щодо предмету спору. Вирішення спору за допомогою такого механізму можливе на будь-якому етапі судового процесу – до того моменту, коли суддя видається в кімнату для винесення судового рішення.

Також, враховуючи євроінтеграційний вектор розвитку України наразі активно впроваджуються альтернативні способи вирішення спорів. Так, 7 серпня 2019 року в Сінгапурі представниками України була підписана Конвенція ООН “Про міжнародні

угоди за результатами медіації”, яка регламентує механізм виконання угод, які були укладені у процесі медіації [5].

З іншого боку, законодавець передбачає можливість досудового врегулювання спору за участю судді. Проте виникає необхідність надання судом роз’яснення учасникам процесу щодо суттєвої різниці між досить схожим інститутом вирішення спору – медіацією та мировою угодою як способом врегулювання спору.

Зокрема, цивільний та господарський процес відносить саме до обов’язку суду роз’яснити можливість для сторін звернутися до суду для врегулювання спору за участю судді. Зокрема, в цьому випадку роз’яснення права на можливість досудового врегулювання спору повинно бути повним та суд повинен пояснити основні відмінності від інших способів досудового врегулювання спору. Можливість звернення до цього механізму вирішення спору можлива лише до початку розгляду справи по суті.

З іншого боку, інститут медіації не є врегульованим, так як відсутнє законодавче закріплення не тільки терміну, а й самого механізму його застосування. Важливо наголосити на тому, що це не є врегулюванням спору за участю судді, з огляду на те, що:

1. Медіація можлива на будь-якій стадії процесу.
2. Здійснюється за допомогою залучення медіатора – посередника, який повинен бути незалежним та мати відповідну освіту.
3. Медіація завжди має дві обов’язкові складові частини – емоційну і предметну. Саме цим медіація відрізняється від судового процесу, який приділяє основну увагу предмету конфлікту. Медіація визнає емоції і дозволяє сторонам їх виражати. Навіть більше, без виходу певної кількості претензій і образ, що накопичилися в обох сторін, і учасникам у край складно шукати взаємоприйнятний вихід із ситуації [6, с. 157].
4. Якщо ж сторони звертаються до вирішення спору за допомогою судді, то буде призначений відповідний суддя, в той же час, сторони мають вільне право самостійно, на власний розсуд обрати медіатора.
5. Є найменш формалізованим та найбільш гнучким процесом, порівнюючи з іншими альтернативними способами вирішення спору. Зокрема, на противагу міжнародному комерційному арбітражу, медіація є більш швидким процесом та потребує менше коштів для реалізації.

На думку Н.О. Волковицької медіація – це метод вирішення спорів із залученням посередника (медіатора), який допомагає проаналізувати конфліктну ситуацію так, щоб зацікавлені сторони самостійно змогли обрати варіант рішення, який задовольняв би інтереси та потреби всіх учасників конфлікту [7].

На противагу цьому, М. Карташов зазначає, що медіація – гнучкий, добровільний і конфіденційний процес, у рамках якого нейтральна третя особа (медіатор) сприяє виробленню сторонами взаємоприйнятного і життєздатного рішення щодо врегулювання спору на умовах взаємної поваги [8, с. 11].

Враховуючи думки вчених, можна визначити, що медіація – це один з альтернативних способів вирішення спорів, який здійснюється шляхом залучення посередника для спільного вироблення сторонами рішення, яке б задовольнило інтереси обох сторін.

Виникає необхідність у законодавчому закріпленні механізму реалізації цього інституту. Указом Президента України від 20.05.15 р. № 276/2015 була схвалена Стратегія реформування судоустрою, судочинства і суміжних правових інститутів на 2015 – 2020 рр., яка передбачає закріплення способів альтернативного врегулювання суперечок шляхом впровадження інституту медіації та посередництва [9].

Важливо наголосити на необхідності роз'яснення суддею сторонам, щодо їх права на альтернативні методи вирішення спору, та оголошення основних відмінностей між 2 способами: медіацією та досудовим врегулюванням спору за участю судді. Тобто необхідність у правовій доступності до інформації для учасників справи – надання інформації учасникам справи щодо їх права вибору (чи бажають сторони застосувати альтернативні способи вирішення спору чи відмовляються від їх застосування), інформування сторін щодо процедури врегулювання спору за допомогою медіації та правових наслідків угоди, укладеної внаслідок застосування медіації. Сторони реалізують право на доступ до інформації – завдяки обізнаності щодо усіх особливостей застосування медіації можливе дійсно ефективне вирішення спору.

Важливим є питання щодо конфіденційності інформації, яку використовували сторони при урегулюванні спору за допомогою посередника. Відповідно до ст. 7 Закону України “Про доступ до публічної інформації” конфіденційна інформація – інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбачених ними умов [10].

Закон вказує, що виключно особа має можливість визначити чи буде інформація конфіденційною або публічною, окрім випадків, встановлених законом.

Відповідно до ч. 2 ст. 70 ЦПК України особи, які не можуть бути допитані як свідки особи, які за законом зобов'язані зберігати в таємниці відомості, що були довірені їм у зв'язку з наданням послуг посередництва (медіації) під час проведення позасудового врегулювання спору. Тобто, медіатор не має можливості розголошення відомостей навіть у якості свідка, що забезпечує конфіденційність інформації отриманої внаслідок проведення посередництва [11].

Відповідно до законопроекту “Про медіацію” від 28.12.19 р. № 2706: “Жодна із сторін медіації, медіатор, інші учасники медіації, а також організація, що забезпечує проведення медіації, не мають права розголошувати інформації, що стосується медіації, без письмової згоди сторін медіації” [12]. Таким чином, передбачається закріплення механізму захисту інформації сторін, за умови, якщо вони не бажають її розголошення.

В багатьох країнах медіація використовується як основний спосіб вирішення спорів. Її застосування умовно можна розподілити на:

1. Обов'язкове досудове застосування для вирішення спору, без можливості відмовитися від її застосування.

2. Обов'язкове застосування, при цьому передбачена можливість сторін відмовитися.

3. Суд зобов'язується рекомендувати сторонам застосувати медіацію, роз'яснює основні правові наслідки її застосування (Велика Британія, Італія, Чеська Республіка) [13].

4. Виключно на власний розсуд сторін врегулювання спору шляхом залучення медіатора. В даному випадку суд не зобов'язаний надавати власні рекомендації або ж звертат увагу на можливість звернення до альтернативних способів вирішення спору.

В цьому аспекті важливо дослідити не тільки міжнародно-правові акти, які регулюють механізм застосування медіації, а й законодавство різних країн. Це зумовлено наявністю різних законодавчих моделей регулювання у зарубіжних країнах

Так, якщо в європейських країнах медіацію можна вважати відносно новим інститутом, то в східних країнах (Китай, Японія, Північна Корея) врегулюванню спору за допомогою посередника надається більша перевага, ніж вирішенню спору шляхом звернення до суду.

Важливо дослідити основні відмінності у доступі до інформації, щодо застосування медіації у Великій Британії, Італії, Азербайджану та Фінляндії.

Основним міжнародно-правовим актом, який закріплює регулювання медіації є Типовий закон ЮНСІТРАЛ про міжнародну комерційну медіацію і міжнародні світові домовленості, укладені під час медіації від 2018 року. Регламентується процедура виконання мирових угод, а також розглядається право сторін посилаючись на мирову угоду у провадженні. У ньому передбачено вичерпний перелік підстав для відмови в наданні засобів правового захисту, на який сторона може посилаючись в рамках провадження, яке підпадає під юрисдикцію Типового закону [14].

Також у зарубіжних країнах по-різному врегульовано питання щодо обов'язковості застосування медіації до початку розгляду справи судом по суті.

Наразі, незважаючи на популярність альтернативних способів вирішення спорів, багато осіб все ж бажають розгляду справи виключно судом. При цьому, суди не можуть примусити сторону до вирішення спору шляхом посередництва, якщо обов'язковість не закріплена на законодавчому рівні.

Також, суд не має юрисдикції зобов'язати сторони вести посередництво проти своєї волі, так як це буде нівелювання норм, закріплених статтею 6 Європейської Конвенції з прав людини. Тому сторони не можуть бути змушені судом вирішувати свої суперечки за допомогою одного з альтернативних способів вирішення спорів, однак прецедентна практика дозволяє судам примусово рекомендувати звернутися до медіації. У Великій Британії у справі *Halsey v Milton Keynes General NHS Trust* висловлювалася позиція щодо форми рекомендації застосування медіації [15]. Це випадок, коли суд досить наполегливо рекомендує сторонам звернутися до медіації, оскільки саме сторони потребують наполегливого заохочення зі сторони судді. Такий підхід у Англії розглядається з двох сторін:

1. Роль суду полягає в тому, щоб заохочувати сторони для вирішення конфлікту, а не примушення до медіації без відповідних правових підстав.

2. Зобов'язання законних представників ознайомити їх клієнтів з перевагами альтернативних способів вирішення спору і надати можливість самостійного вибору способу вирішення спору.

Тобто вирішується питання щодо розмежувань повноважень суду і представників у питанні зобов'язання щодо рекомендації застосування альтернативних способів вирішення спору.

Виходячи з положень таких документів як Правила цивільного судочинства, *Pre-action protocols* (Протоколи, що пояснюють поведінку та визначають кроки, які сторони повинні вжити перед початком провадження конкретних видів цивільних позовів, вони додаються відповідно до Правил цивільного судочинства (CPR – Civil Procedure Rules)), *TeCSA ADR Protocol* (Протокол, що передбачає використання альтернативного способу вирішення спорів, звертаючись до Технологічного та будівельного суду у судових, арбітражних та інших процедурах, де це доречно та потенційно вигідно сторонам у контексті суперечки між ними) закріплюють такі положення:

- Суд надаватиме заохочення сторонам використовувати альтернативне вирішення спорів і, коли це доцільно, полегшить використання такої процедури.

- Юридичні представники у всіх випадках повинні гарантувати, що їхні клієнти повністю усвідомлюють переваги ADR.

- Альтернативні способи вирішення спорів може бути доцільним до початку розгляду справи або на будь-якій стадії [16].

Можна дійти до висновку, що повідомлення учасників процесу повинно здійснюватися з обов'язковою рекомендацією судді реалізувати механізм застосування медіації (у випадку, якщо це сприятиме оперативному та ефективному вирішенню спору), та при роз'ясненні представниками усіх переваг і недоліків вирішення спору шляхом залучення посередника. Саме такий спосіб застосування зумовлений тим фактом, що судові провадження займає багато часу, судові процеси часто є складними та економічно неефективними, в свою чергу залучення професійного посередника може забезпечити врегулювання спору досить швидко.

Все це зумовлює забезпечення законодавством Великої Британії права на доступ до інформації при альтернативних способах вирішення спору як від судді, так і від законних представників, і таким чином надає сторонам право реалізувати альтернативні механізми для захисту своїх прав.

Відповідно до Директиви Європейського Союзу № 2008/52/ЄС передбачається добровільне застосування медіації сторонами, проте держава може законодавчо закріпити випадки для яких категорій справ вона є обов'язковою [17].

Зокрема, імплементацію цього положення можна дослідити на досвіді Італії. Для цього було прийнято Декрет № 28/2010 [18], який закріпив основні положення Директиви, процедуру повідомлення судом сторін щодо можливості застосування медіації та процесу її проведення. Варто зауважити, що в Італії медіацію розділяють на обов'язкову та добровільну:

За умови застосування добровільної медіації суд лише зобов'язаний повідомити сторони про альтернативний спосіб урегулювання спору.

Застосування обов'язкової медіації передбачається законом перед поданням позовної заяви до суду. Це стосується сімейних правовідносин, позику, оренди, страхування та інших категорій справ передбачених Декретом від 08.10.07 р. № 179 [19].

В аспекті самої процедури проведення медіації цікаво дослідити процедуру проведення медіації, яка включає у себе важливий аспект реалізації права на доступ до інформації. Сторони повинні брати участь у медіації з обов'язковим представництвом адвоката. При цьому медіатор зобов'язаний роз'яснити сторонам та адвокатам функцію та порядок проведення медіації. Завдяки цьому забезпечується належне проведення медіації так як сторони та адвокати ознайомлені з процедурою і можуть належним чином вирішити спір. Після роз'яснення медіатор розпочинає здійснювати посередництво і сторони безпосередньо можуть вирішити спір.

У Фінляндії медіація здійснюється на добровільній основі за заявою сторін у цивільному та кримінальному процесі. Виключно за згодою усіх сторін суд може прийняти рішення про початок судової медіації.

Якщо в Великій Британії суд зобов'язується роз'яснити необхідність звернення до альтернативних способів вирішення спору, то у Фінляндії відповідно до Розділу 4 Закону про посередництво сторони самостійно повинні надати підстави для проведення медіації [20].

Фінське законодавство також передбачає обов'язок сторони повідомити другу сторону щодо ініціювання медіації. Якщо ж не було здійснено повідомлення заздалегідь, то це здійснюється у судовому процесі безпосередньо, що забезпечує рівний доступ сторін до інформації та можливість обрати спосіб урегулювання спору з урахуванням позиції обох сторін. Перш ніж сторони погодяться на медіацію, їм має бути роз'яснено судом їх права, порядок висловлення позиції в процесі погоджувальної процедури та можливість відмовитися від медіації на будь-якій стадії розгляду шляхом звернення до медіатора.

Відповідно до законодавства Азербайджану, а саме Law of Republic Azerbaijan on Mediation, Article 29.1 у початковій сесії медіації медіатор зобов'язаний пояснити суть, переваги та правила медіаційного процесу, та надати сторонам право продовження процедури медіації в той же день або ж призначити розгляд в інший день [21].

Зазвичай судді рекомендують сторонам здійснити на посередництво на ранніх стадіях судового провадження. Завдяки цьому сторони можуть не витрачати велику кількість часу на судовий процес, так як будуть ознайомлені з основними перевагами застосування медіації вже на першому судовому засіданні.

Наприклад, у Бельгії суддя, якщо він вважає, що примирення між сторонами можливе, суддя може за власною ініціативою чи на вимогу однієї із сторін доручити посередництво після заслуховування сторін під час вступного слухання або слухання про розгляд справи по суті. Це зумовлене тим, що на цій ранній стадії суддя може бути не повністю ознайомлений зі сторонами та розглянутою справою. Більше того, позиції сторін та готовність до врегулювання можуть змінитися під час судового розгляду. Таким чином, суддя має видати ухвалу, яка вимагає від сторін застосувати посередництво на будь-якій стадії провадження до прийняття рішення [22].

В даному випадку суд самостійно, на власний розсуд вирішує чи доцільно застосування медіації – при цьому право особи на інформацію, щодо процесу медіації, її прав та загалом підстав для застосування медіації суддею реалізується. Тоді приймає відповідний процесуальний документ (наказ або ухвалу) на будь-якій стадії розгляду, у якому пояснює основні підстави для реалізації медіації між сторонами.

Висновки.

Підводячи підсумки, можна стверджувати, що роз'яснення можливості застосування альтернативних способів врегулювання спорів є проявом права на доступ до інформації. Це зумовлено тим, що суддя зобов'язується надати сторонам інформацію щодо можливості застосування посередництва для врегулювання спору, незалежно від того, чи є медіація у країні обов'язковою або добровільною.

Проведений аналіз законодавства зарубіжних країн дає підстави сформулювати основні напрями вдосконалення доступу до інформації при альтернативних методах вирішення спорів, які передбачають:

законодавче закріплення добровільної медіації та вдосконалення існуючих механізмів доступу до інформації щодо медіації. Це можливо реалізувати внесенням відповідних змін до процесуальних кодексів, а саме щодо обов'язку суду рекомендувати сторонам звернутися до медіації;

необхідність визначення у законодавстві понять “медіація” та “врегулювання спору за участю судді”;

здійснення імплементації норм Сінгапурської Конвенції 2018 року до законодавства України для регламентації процедури посередництва.

Використана література

1. Venice Commission. The Rule of Law. Venice, 2016. URL: [https://www.venice.coe.int/web-forms/documents/?pdf=CDL-AD\(2016\)007-e](https://www.venice.coe.int/web-forms/documents/?pdf=CDL-AD(2016)007-e)
2. OpenDataBot – найбільш завантажений суд в Україні. – 2017. URL: <https://www.opendatabot.ua/blog/35-fast-court>
3. Статистика надходження справ Верховного Суду України. URL: <https://www.facebook.com/101352490639645/posts/641932343248321/?d=n>
4. Господарський процесуальний кодекс України: Закон України. *Відомості Верховної Ради України*. 1992. № 6. Ст. 56. URL: <https://www.zakon.rada.gov.ua/laws/show/1798-12>

5. United Nations Convention on International Settlement Agreements Resulting from Mediation (the “Singapore Convention on Mediation”). URL: https://www.uncitral.un.org/en/texts/mediation/conventions/international_settlement_agreements

6. Катаєва Е. Національні особливості медіації в Україні. Досвід та перспективи. *Слово національної школи суддів України*. 2013. № 3. С. 156-161.

7. Волковицька Н.О. Медіація: альтернативний чи ефективний спосіб вирішення спорів. URL: <http://www.yur-gazeta.com/publications/practice/inshe/mediaciya-alternativniy-chi-efektivniysp-osib-virishennya-sporiv.html>

8. Карташов М. Медіація як форма вирішення корпоративних спорів. *Підприємництво, господарство і право*. 2019. № 10.

9. Про Стратегію реформування судоустрою, судочинства та суміжних правових інститутів на 2015 – 2020 роки: Указ Президента України від 20.05.15 р. № 276/2015. URL: <https://www.zakon.rada.gov.ua/laws/show/276/2015>

10. Про доступ до публічної інформації: Закон України. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314. URL: <https://www.zakon.rada.gov.ua/laws/show/2939-17>

11. Цивільний процесуальний кодекс України: Закон України. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст. 492. URL: <https://www.zakon.rada.gov.ua/laws/show/1618-15>

12. Про медіацію: проект закону України від 28.12.19 р. № 2706. URL: http://www.search.ligazakon.ua/l_doc2.nsf/link1/JI01110A.html

13. Національна асоціація медiatorів України. Медіація у світі. – 2016. URL: <http://www.namu.com.ua/ua/info/mediation/in-the-world>

14. UNCITRAL Model Law on International Commercial Mediation and International Settlement Agreements Resulting from Mediation, 2018. URL: https://www.uncitral.un.org/en/texts/mediation/modellaw/commercial_conciliation

15. Halsey v Milton Keynes General NHS Trust [2004] EWCA Civ 576 (11 May 2004). URL: [https://www.uk.practicallaw.thomsonreuters.com/D-000-4986?transitionType=Default&contextData=\(sc.De fault\)&firstPage=true&bhcp=](https://www.uk.practicallaw.thomsonreuters.com/D-000-4986?transitionType=Default&contextData=(sc.De fault)&firstPage=true&bhcp=)

16. Jeremy Glover, Fenwick Elliott. Mediation: is it ever reasonable to decline a request to mediate? 2015. URL: <https://www.fenwickelliott.com/research-insight/articles-papers/alternative-dispute-resolution/mediation-decline-request-mediate>

17. Про деякі аспекти посередництва (медіації) в цивільних та комерційних справах: Директива № 2008/52/ЄС Європейського Парламенту і Ради. URL: https://www.zakon.rada.gov.ua/laws/show/994_a95

18. Mediazione: il DLgs. n. 28/2010 aggiornato con al Decreto del Fare. URL: https://www.altalex.com/documents/news/2013/08/05/mediazione-il-dlgs-n-28-2010-aggiornato-con-al-decreto-del-fare#_Toc36063542

Risparmio: procedure di conciliazione, arbitrato, indennizzo e fondo di garanzia Decreto legislativo, 08/10/2007 n° 179, G.U. 30/10/2007. URL: <https://www.altalex.com/documents/leggi/2007/11/07/risparmio-procedure-di-conciliazione-arbitrato-indennizzo-e-fondo-di-garanzia>

Laki riita-asioiden sovittelusta ja sovinnon vahvistamisesta yleisissä tuomioistuimissa – 294. URL: <https://www.finlex.fi/fi/laki/ajantasa/2011/20110394#L2>

Law of Republic Azerbaijan on Mediation. URL: <http://www.justice.gov.az/senedler/49?Culture=en., article 29.1>

Kingdom of Belgium, Judicial Code Moniteur Belge. URL: <http://www.epej-2019-9-en-handbook/1680951928>

~~~~~ \* \* \* ~~~~~

УДК 34:378(477)

МАНЬГОРА В.В., кандидат педагогічних наук, доцент,  
професор кафедри права “ПрАТ “ВНЗ “МАУП”

## ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ЮРИДИЧНОЇ ОСВІТИ

**Анотація.** В статті досліджуються особливості інформаційно-правового забезпечення юридичної освіти на сучасному етапі в Україні. Здійснено аналіз чинного законодавства що регулює інформаційно-правове забезпечення юридичної освіти. Визначено основні проблеми інформаційно-правового забезпечення юридичної освіти та розроблено пропозиції щодо вдосконалення підготовки майбутніх юристів.

**Ключові слова:** інформаційно-правове забезпечення, інформаційне забезпечення, правове забезпечення, освіта, юридична освіта.

**Summary.** Special features of information and legal support of legal education at the present stage in Ukraine are provided in the article. The current legislation regulating the information and legal support of legal education has been analyzed. The main problems of information and legal support of legal education are identified and proposals for improving the training of future lawyers are developed.

**Keywords:** information and legal support, information support, legal support, education, legal education.

**Аннотация.** В статье исследуются особенности информационно-правового обеспечения юридического образования на современном этапе в Украине. Осуществлен анализ действующего законодательства регулирующего информационно-правовое обеспечение юридического образования. Определены основные проблемы информационно-правового обеспечения юридического образования и разработаны предложения по совершенствованию подготовки будущих юристов.

**Ключевые слова:** информационно-правовое обеспечение, информационное обеспечение, правовое обеспечение, образование, юридическое образование.

**Постановка проблеми.** Глобальні процеси інформатизації суспільства вимагають ефективного інформаційно-правового забезпечення юридичної освіти. Професійна діяльність юриста в умовах інформаційного суспільства залежить від його здатності адаптуватися до сучасних умов. Підготовка конкурентоздатних фахівців в галузі права вимагає освоєння і використання ними нормативно-правового забезпечення та інформаційно-комунікаційних технологій.

Свідченням надзвичайної важливості реформи юридичної освіти в сьогоденних умовах є створення робочої групи з питань розвитку юридичної освіти у складі Комісії з правової реформи при Президентові України, що затверджена Указом Президента України у липні 2019 року.

Реформа юридичної освіти проводиться Міністерством освіти і науки та Міністерством юстиції, оскільки ціла низка нормативно-правових актів визначає їх відповідальними за впровадження окремих складових реформи юридичної освіти [1].

На сайті Комітету Верховної Ради з питань науки, освіти та інновацій був опублікований 26 лютого 2020 р. новий проект Концепції розвитку юридичної освіти, який розроблений та обговорений на робочих зустрічах народних депутатів України спільно з експертами у галузі права та вищої освіти [2].

**Результати аналізу наукових публікацій.** Питання інформаційно-правового забезпечення висвітленні в працях О. Баранова, В. Брижка, В. Горового, Н. Савінової, В. Фурашева, Л. Хромченко та інших.

Проблемі інформатизації освіти присвячені праці В. Бикова, А. Гуржія, А. Іваннікова, Ю. Іжванова, О. Кривошеева, Т. Кронівець, О. Мойко, С. Ніколаєнка, Л. Полякової, Р. Шевчука.

Методику формування інформативних компетентностей у майбутніх юристів на дисертаційному рівні досліджували: Н. Русіна [3], О. Федорчук [4]. Питання інформаційно-правового забезпечення юридичної освіти потребують окремого дослідження.

**Метою статті** є визначення особливостей інформаційно-правового забезпечення юридичної освіти, виявлення основних проблем інформаційно-правового забезпечення юридичної освіти та розробка пропозицій щодо вдосконалення підготовки юристів.

**Виклад основного матеріалу.** Інформаційно-правове забезпечення визначається як сукупність управлінських прийомів у системі управління, спрямованих на формування необхідної інформації, спеціальних методів її обробки, систематизації, групування [1, с. 112].

Аналітичний огляд нормативно-законодавчої бази України з питань інформаційно-правового забезпечення дає підстави відзначити, що на цей час діє 260 законів України, 290 постанов Верховної Ради України нормативного змісту, 375 указів і 87 розпоряджень Президента України, 1 160 постанов та 210 розпоряджень Кабінету Міністрів та більше 1 000 нормативних актів, що регулюють правовідносини в країні [5, с. 156].

Нормативно-правові акти інформаційно-правового забезпечення юридичної освіти за рівнем правого регулювання можна класифікувати на міжнародно-правові та національні.

Основними міжнародно-правовими актами інформаційно-правового забезпечення юридичної освіти є Загальна декларація прав людини, Міжнародний пакт про громадянські та політичні права, Конвенція про захист прав людини і основоположних свобод, Конвенція про правову допомогу та правові відносини у цивільних, сімейних та кримінальних справах, Рекомендація Комітету Міністрів Ради Європи № R(2000)21 про свободу професійної діяльності адвоката, Рекомендація Комітету Міністрів Ради Європи № R(2000)19 про роль публічного обвинувача в системі кримінальної юстиції, Рекомендація Комітету Міністрів Ради Європи № R(2004)4 про Європейську Конвенцію з прав людини в університетській освіті та професійному навчанні, Спільною декларацією про Європейський простір вищої освіти, прийняту в Болоньї 19 червня 1999 року, Рекомендація Комітету Міністрів Ради Європи № R(2000)8 про дослідницьку місію університетів, Рекомендація Комітету Міністрів Ради Європи № R(2007)6 про відповідальність держави за вищу освіту та наукові дослідження.

Нормативно-правове забезпечення підготовки майбутніх юристів в Україні відбувається на основі правових норм Конституції України від 28 червня 1996 року; Законів України: “Про освіту” від 05 вересня 2017 року № 2145-VIII, “Про вищу освіту” від 01 липня 2014 року № 1556-VII, “Про наукову і науково-технічну діяльність” від 26 листопада 2015 року № 848-VIII; Постанов Кабінету Міністрів України: “Про Державну національну програму “Освіта” (“Україна XXI століття”) від 3 листопада 1993 року № 896, “Про затвердження Програми розвитку юридичної освіти на період до 2005 року” від 10 квітня 2001 р. № 344, “Про затвердження національної рамки кваліфікацій” від 23 листопада 2011 року № 1341, “Про затвердження переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти” від 29

квітня 2015 року № 266, “Про затвердження переліку спеціальностей, за якими проводиться єдиний державний кваліфікаційний іспит для здобуття ступеня магістра” від 10 травня 2018 року № 354, “Порядок атестації осіб, які здобувають ступінь магістра, у формі єдиного державного кваліфікаційного іспиту” від 17 липня 2019 року № 684; Указів Президента України: “Про національну стратегію розвитку освіти в Україні на період до 2021 року” від 25 червня 2013 р. № 344/2013, “Про цілі сталого розвитку до 2030 року” від 30 вересня 2019 р.; наказів Міністерства освіти і науки України: “Про затвердження стандарту вищої освіти України за спеціальністю 081 “Право” галузі знань 08 “Право” для першого (бакалаврського) рівня вищої освіти” наказом Міністерства освіти і науки України № 1379 від 12 грудня 2018 року, “Про утворення робочої групи з розроблення Концепції розвитку юридичної освіти в Україні” № 787 від 5 липня 2016 року, “Методичні рекомендації щодо розроблення стандартів вищої освіти” від 1 червня 2016 року.

Останнім часом було розроблено проекти нормативно-правових актів: проект Закону України “Про юридичну (правничу) освіту і загальний доступ до правничої професії” від 28 вересня 2017 р. №7147, проект Закону про юридичну освіту та юридичну (правничу) професію від 17 жовтня 2017 р., які мали сприяти реформуванню підготовки юристів. Проекти законів було відхилено 29 серпня 2019 р.

У рамках реформування системи вищої освіти та комплексного оновлення законодавства у цій сфері, нагальним і позитивним кроком І. Тимкович вважає прийняття Міністерством освіти і науки України наказу від 05.07.2016 р. № 787 “Про утворення робочої групи з розроблення Концепції розвитку юридичної освіти в Україні”, обговорення шляхів удосконалення її правових і організаційних засад за участі не лише представників органів державної влади, але й партнерів, котрі реалізують проект USAID “Справедливе правосуддя”, координаторів проектів ОБСЄ в Україні, представників вищих навчальних закладів та громадських об’єднань. Відповідно до наказу, перед робочою групою поставлено завдання до 30 вересня 2016 р. розробити та подати на погодження до Міністерства освіти і науки України проект Концепції розвитку юридичної освіти в Україні, а до 30 грудня 2016 р. розробити та подати на погодження до вказаного міністерства проект Плану реалізації даної Концепції. Результатом цієї роботи стала презентація Міністром освіти і науки України, головою робочої групи з розробки концепції Лілією Гриневич та заступником Міністра юстиції України Ганною Онищенко Концепції вдосконалення правничої (юридичної) освіти для фахової підготовки правника відповідно до європейських стандартів вищої освіти та правничої професії, проведена 14 вересня 2016 р. під час круглого столу “Модернізація правничої освіти в Україні”, а текст проекту Концепції розміщений на сайті Міністерства освіти і науки України для ознайомлення громадськості [6, с. 56].

Концепція розвитку юридичної освіти розроблена для забезпечення якості вищої юридичної освіти та перевірки відповідності здобутих результатів навчання випускників потребам ринку праці, сучасним викликам глобалізованої правничої професії та найкращим світовим практикам. Необхідно забезпечити ефективне функціонування внутрішньої та зовнішньої систем забезпечення якості вищої освіти [7].

Інформаційно-правовими елементами системи внутрішнього забезпечення якості підготовки правників відповідно до проекту Концепції розвитку юридичної освіти є:

- наявність інформаційних систем для ефективного управління освітнім процесом;
- публічність інформації про освітні програми та кваліфікації;
- дотримання академічної доброчесності працівниками закладів вищої освіти та здобувачами вищої юридичної освіти, у тому числі створення і забезпечення

функціонування ефективної системи запобігання та виявлення плагіату та інших проявів академічної недоброчесності;

- створення дієвої системи відповідальності за недотримання вимог академічної доброчесності;

- забезпечення для здобувачів вищої юридичної освіти доступу до навчальних ресурсів, зокрема визнаних професійних баз даних, міжнародних інформаційних, науково-практичних, бібліотечних та інших ресурсів [7].

Важливим кроком до трансформації існуючої системи юридичної освіти, на думку Л. Столярчук, стало затвердження Стандарту вищої освіти України за спеціальністю 081 “Право” галузі знань 08 “Право” для першого (бакалаврського) рівня вищої освіти наказом Міністерства освіти і науки України від 12 грудня 2018 року № 1379. Цей стандарт вводився в дію з 2018/2019 навчального року та визначає базові вимоги до змісту та результатів освітньої діяльності ЗВО, які готують бакалаврів права. Зокрема, даний документ надає перелік компетентностей випускника, які представлені 3 видами: інтегральна компетентність, загальні та спеціальні (фахові, предметні) компетентності. Крім того, представлений нормативний зміст підготовки бакалаврів права, сформульований у термінах результатів навчання, які включають такі блоки: соціально-гуманітарна ерудованість, дослідницькі навички, комунікація, професійна самоорганізація та використання інформаційних технологій, праворозуміння та правозастосування [8, с. 91].

Активною є співпраця Міністерства освіти та науки України та Міністерства юстиції України щодо реформування юридичної освіти. У структурі Міністерств за формування державної політики у сфері юридичної освіти відповідають Директорати – Директорат вищої освіти та освіти дорослих МОН, а також Директорат з прав людини, доступу до правосуддя та правової обізнаності Мін'юсту.

За останні роки завдяки спільним діям обох міністерств, за активного сприяння міжнародних партнерських організацій, професійних правничих спільнот, вдалося суттєво просунутися в цьому напрямку, зокрема в питаннях концептуального нормотворення, вдосконалення відбору на навчання у правничі школи, оптимізації державного замовлення на підготовку фахівців з юридичною освітою, рекомендацій щодо покращення змісту освітніх програм тощо [9].

Новий проект концепції розвитку юридичної освіти, який розроблений та обговорений на робочих зустрічах народних депутатів України спільно з експертами у галузі права та вищої освіти, передбачає віднесення до вищої юридичної освіти вищої освіти ступеня магістра за спеціальністю 081 “Право” галузі знань 08 “Право”. Ступінь магістра за спеціальністю 081 “Право” здобувається на основі повної загальної середньої освіти. Також встановлено, що підготовка здобувачів освіти за спеціальністю 081 “Право” в системі фахової передвищої освіти та за ступенем молодшого бакалавра та бакалавра не здійснюється [10].

Спеціальності “Міжнародне право” та “Правоохоронна діяльність” не вважатимуться вищою юридичною освітою в контексті кваліфікаційних вимог для зайняття певної посади.

Скасовується можливість заочної форми навчання: підготовка правників здійснюватиметься виключно за денною формою здобуття освіти [11].

На думку авторів проекту, Концепція розвитку юридичної освіти має відповідати положенням стратегічних та програмним документів, зокрема: Національній Стратегії в сфері прав людини, Стратегії реформування судоустрою, судочинства та суміжних

правових інститутів на 2015 – 2020 роки, Концепції підготовки фахівців за дуальною формою здобуття освіти, Концепції розвитку громадянської освіти в Україні.

Концепція розвитку юридичної освіти передбачає:

- сприяння збільшенню необхідних ресурсів для організації освітнього процесу, у тому числі самостійної роботи студентів;
- наявність інформаційних систем для ефективного управління освітнім процесом;
- забезпечення для здобувачів юридичної освіти доступу до навчальних ресурсів, зокрема визнаних професійних баз даних, міжнародних інформаційних, науково-практичних, бібліотечних та інших ресурсів [10].

Проект концепції юридичної освіти з метою забезпечення якості підготовки правників передбачає організацію та проведення Єдиного державного кваліфікаційного іспиту.

17 липня 2019 р. Кабінет Міністрів України видав постанову “Порядок атестації осіб, які здобувають ступінь магістра, у формі єдиного державного кваліфікаційного іспиту” [12]. У цьому Порядку під терміном “єдиний державний кваліфікаційний іспит” розуміється стандартизована форма контролю досягнення здобувачем вищої освіти результатів навчання, визначених стандартом вищої освіти, та оцінювання таких результатів навчання.

Атестація осіб, які здобувають ступінь магістра, у формі кваліфікаційного іспиту здійснюється за спеціальностями згідно з переліком спеціальностей, за якими проводиться єдиний державний кваліфікаційний іспит для здобуття ступеня магістра, затвердженим постановою Кабінету Міністрів України від 10 травня 2018 року № 354 [13].

Державними органами відповідальними за організацію кваліфікаційного іспиту за спеціальністю 081 “Право” є Міністерство освіти і науки та Міністерство юстиції.

Відповідно до постанови Кабінету Міністрів України “Порядок атестації осіб, які здобувають ступінь магістра, у формі єдиного державного кваліфікаційного іспиту” програми кваліфікаційного іспиту розробляються на основі стандартів вищої освіти відповідного рівня та спеціальності. Але на жаль стандарт вищої освіти України: другий (магістерський) рівень вищої освіти, галузь знань 08 “Право”, спеціальність 081 “Право” не прийнятий, хоч на сайті Міністерства освіти і науки є розроблений проект.

Програма єдиного державного кваліфікаційного іспиту за спеціальністю 081 “Право” (магістерський рівень вищої освіти) не оприлюднена на офіційних веб-сайтах, хоча 7 листопада 2019 р. за наказом Міністра освіти і науки Г. Новосад було створено робочу групу з питань методичного, організаційного та аналітичного забезпечення єдиного державного кваліфікаційного іспиту за спеціальностями 081 “Право” та 293 “Міжнародне право”.

Підготовка конкурентоздатних фахівців в галузі права вимагає освоєння і використання ними інформаційно-комунікаційних технологій.

Інформаційно-комунікаційні технології – це сукупність методів, засобів та прийомів пошуку, зберігання, опрацювання, подання та передавання графічних, текстових, цифрових, аудіо та відеоданих на базі персональних комп’ютерів, комп’ютерних мереж та засобів зв’язку [14, с. 195].

ІКТ здійснюють активний вплив на процес навчання і виховання студентів, оскільки змінюють схему передавання знань і методи навчання.

Основними засобами ІКТ, які застосовуються у навчально-виховному процесі майбутніх юристів є: текстові і табличні процесори, комп’ютерні презентації, електронні довідники, електронні підручники і мультимедіа; електронні бібліотеки й архіви, експертні та інформаційно-пошукові (універсальні) системи, банки і бази даних,

глобальні та локальні освітні мережі, хмарні технології. Вони допомагають майбутньому юристу вибрати необхідну інформацію та належним чином її представити.

### **Висновки.**

Інформаційно-правове забезпечення юридичної освіти – це сукупність нормативно-правових актів та інформаційно-комунікативних технологій, які використовуються при підготовці майбутніх юристів.

Реформи юридичної освіти неможливі без прийняття Концепції розвитку юридичної освіти та механізму її реалізації, без прийняття стандарту вищої освіти України: другий (магістерський) рівень вищої освіти, галузь знань 08 “Право”, спеціальність 081 “Право” та розробки єдиного державного кваліфікаційного іспиту. Тому необхідно прийняти нормативно-правові акти, які відповідають сучасним вимогам та міжнародним стандартам підготовки майбутніх юристів.

### **Використана література**

1. Хромченко Л.Г., Раковська-Башмакова О.С., Шраср А.С. Організація інформаційної діяльності. Теоретичні основи: навч. посібник; за заг. ред. Х.В. Чаловського. Харків: МСУ, 2008. 351 с.
2. Проект Концепції вдосконалення юридичної освіти представлено суспільству. – (Міністерство освіти і науки України від 15.09.2016 р.). URL: [http://www.kmu.gov.ua/control/uk/publish/article?art\\_id=249321194&cat\\_id=244277212](http://www.kmu.gov.ua/control/uk/publish/article?art_id=249321194&cat_id=244277212) (дата звернення 09.03.2020).
3. Русіна Н.Г. Методика формування інформативних компетентностей у майбутніх правознавців: автореф. дис. ...канд. пед. наук: 13.00.02 “Теорія та методика навчання”. Київ, 2016. 20 с.
4. Федорчук О.С. Формування у майбутніх правознавців навичок професійного застосування інформаційно-комунікаційних технологій: автореф. дис. ...канд. пед. наук: 13.00.04 “Теорія і методика професійної освіти”. Київ, 2009. 20 с.
5. Павліченко Є. Напрями удосконалення інформаційно-правового забезпечення суб’єктів господарювання. *Підприємництво, господарство і право*. 2017. № 3. С.155-158.
6. Тимкович І.І. Юридична освіта як елемент правової системи України. *Юридичний вісник*. 2016. № 4(41). С.54-58.
7. Проект Концепції розвитку юридичної освіти. URL: <https://www.mon.gov.ua/ua/osvita/visha-osvita/koncepciya-vdoskonalennya-pravnichoyi-yuridichnoyi-osviti-dlya-fahovoyi-pidgotovki-pravni-ka> (дата звернення 09.03.2020).
8. Столярчук Л.Б. Сучасний стан професійної підготовки бакалаврів права в закладах вищої освіти України. *Молодий вчений*. 2019. № 1(65). С. 89-94.
9. Шемелинець І. Точка біфуркації: курс на продовження реформи юридичної освіти. *Юридична газета online*. № 43-44 (697-698). URL: <https://www.yur-gazeta.com/publications/practice/inshe/tochka-bifurkaciyi-kurs-na-prodovzhennya-reformi-yuridichnoyi-osviti.html> (дата звернення 09.03.2020).
10. Проект Концепції розвитку юридичної освіти. URL: <http://www.kno.rada.gov.ua/print/75465.html> (дата звернення 09.03.2020).
11. Реформа юридичної освіти: головні тези проекту. URL: <https://www.pravo.ua/reforma-juridichnoyi-osviti-golovni-tezi-proektu/> (дата звернення 09.03.2020).
12. Порядок атестації осіб, які здобувають ступінь магістра, у формі єдиного державного кваліфікаційного іспиту від 17.07.19 р. № 684. URL: <https://www.zakon.rada.gov.ua/laws/show/684-2019-%D0%BF> (дата звернення 09.03.2020).
13. Про затвердження переліку спеціальностей, за якими проводиться єдиний державний кваліфікаційний іспит для здобуття ступеня магістра: Постанова Кабінету Міністрів України від 10.05.18 р. № 354. URL: <https://www.zakon.rada.gov.ua/laws/show/354-2018-%D0%BF> (дата звернення 09.03.2020).

14. Маньгора В.В. Формування інформаційної компетентності майбутніх юристів у процесі фахової підготовки: матеріали наук.-практ. конф. *Теоретико-правові основи формування та розвитку інформаційного суспільства*, м. Київ, 29 лист. 2017 р. / упоряд. В.М. Фурашев, С.Ю. Петряєв. – (Нац. техн. ун-т України “КПІ ім. Ігоря Сікорського”). Київ: “Політехніка”, 2017. С. 192-196.

15. Концепція вдосконалення правової (юридичної) освіти для професійної підготовки юриста відповідно до європейських стандартів вищої освіти і юридичної професії. URL: <https://www.mon.gov.ua/ua/osvita/visha-osvita/koncepciyavdoskonalennya-pravnichoyi-yuridichnoyi-osviti-dlyaafahovoyi-pidgotovki-pravnika>. (дата звернення 09.03.2020).

16. Концепція реформи юридичної освіти пропонує впровадити “наскрізну” магістерку для правників. URL: <http://www.ukrainepravo.com/news/ukraine> (дата звернення 09.03.2020).

17. Про утворення робочої групи з розроблення концепції розвитку юридичної освіти в Україні: наказ Міністерства освіти і науки України від 05.07.16 р. № 787 URL: <http://www.old.mon.gov.ua/ua/aboutministry/normative/5737> (дата звернення 09.03.2020).

18. Семенець-Орлова І.А. Нормативно-правове забезпечення освітніх змін в Україні. Теорія та практика державного управління. 2017. № 3(58). С. 1-10.

~~~~~ \* \* \* ~~~~~

УДК 349.412.2(477)

МАНЬГОРА Т.В., кандидат юридичних наук, старший викладач кафедри права
Вінницького Національного аграрного університету.

НАБУВАЛЬНА ДАВНІСТЬ НА ЗЕМЕЛЬНУ ДІЛЯНКУ

Анотація. Інститут набувальної давності на земельну ділянку в земельному законодавстві запроваджено більше сімнадцяти років тому, але до сьогодні немає однозначного розуміння даної проблеми. Автор дослідив інститут набувальної давності у Цивільному та Земельному кодексах України та окреслив особливості застосування набувальної давності по відношенню до земельної ділянки. Потенційним суб'єктом набувальної давності на земельну ділянку в Україні може бути лише громадянин. Відкритим залишається питання щодо можливості розширення кола суб'єктів, які внаслідок набувальної давності можуть набувати земельні права на конкретну земельну ділянку. Охарактеризовано основні ознаки набувальної давності: володіння є добросовісним; володіння визнається відкритим; володіння визнається безперервним. Визначено основні шляхи вдосконалення дієвості інституту набувальної давності земельної ділянки.

Ключові слова: набувальна давність, право власності на землю, давність користування, набуття права власності, добросовісність володіння, відкритість володіння, безперервність володіння.

Summary. The institute of land prescription time in Land Law has been introduced for over seventeen years, but to date there is no unambiguous understanding of this problem. The author examined the institute of land prescription time in the Civil and Land Codes of Ukraine and outlined the peculiarities of using the prescription time with regard to the land plot. Only a citizen can be a potential subject of the prescription time on land in Ukraine. The question remains as to the possibility of expanding the range of entities which, as a result of the land prescription time, may acquire land rights to a particular land plot. The main features of the statute of the land prescription time are characterized: the ownership is conscientious; the possession is recognized as opened; the ownership is recognized as continuous. The main ways of improving the efficiency of the land acquisition prescription time have been determined.

Keywords: anacquisitive prescription time, land ownership, prescription of use, an acquisition of property rights, a possession in good faith.

Аннотация. Институт приобретательной давности на земельный участок в земельном законодательстве введен более семнадцати лет назад, но до сих пор нет однозначного понимания данной проблемы. Автор исследовал институт приобретательной давности в Гражданском и Земельном кодексах Украины и очертил особенности применения приобретательной давности в отношении земельного участка. Потенциальным субъектом приобретательной давности на земельный участок в Украине может быть только гражданин. Открытым остается вопрос о возможности расширения круга субъектов, которые вследствие приобретательной давности могут приобретать земельные права на конкретный земельный участок. Охарактеризованы основные признаки приобретательной давности: владение является добросовестным; владение признается открытым; владение признается непрерывным. Определены основные пути совершенствования действенности института приобретательной давности земельного участка.

Ключевые слова: приобретаемая давность, право собственности на землю, давность пользования, приобретение права собственности, добросовестность владения, открытость владения, непрерывность владения.

Постановка проблеми. Земельний кодекс України, який набрав чинності 1 січня 2002 р., вперше закріпив низку нових принципових положень, яких раніше не було в земельному законодавстві. Серед таких новел окреме місце посідає набувальна давність, тобто набуття права на земельну ділянку за давністю користування. Відповідні правові приписи, що регулюють набувальну давність на земельну ділянку, містяться у ст. 119 Земельного кодексу України [1]. На даний час земельне законодавство пропонує неоднозначне розуміння регулювання інституту набувальної давності на земельну ділянку, що потребує нових досліджень, аналізу практики розв'язання спорів після 1 січня 2017 р. з метою виправлення недоліків та пошуку шляхів вдосконалення даного інституту.

Результати аналізу наукових публікацій. Дослідженням проблеми набуття права на земельну ділянку за набувальною давністю займалися Я. Білий [2], Ю. Брикайло [3], К. Дудник [4], В. Любич [5], Р. Марусенко [6], А. Мірошніченко [7], Л. Решетник [8], К. Рибалко [9], А. Ріпенко [10], Б. Фасій [11], А. Федорченко [12], Н. Черкаська [13], М. Шульга [14]. На рівні дисертаційних робіт частково проблеми набуття права на земельну ділянку за набувальною давністю досліджували С. Губарєв “Право власності фізичної особи на присадибну земельну ділянку (садиби)” [15], В. Маковій “Набувальна давність у цивільному праві” [16], І. Панченко “Визнання права власності як спосіб захисту цивільних прав” [17], О. Стаценко “Набуття права власності на нерухоме майно за набувальною давністю” [18].

Метою статті є дослідження проблеми набуття права на земельну ділянку за набувальною давністю, з метою виявлення недоліків та напрацювання пропозицій щодо їх усунення.

Виклад основного матеріалу. Земля завжди відігравала визначальну роль в переліку нерухомих речей. Саме тому, на нашу думку, законодавець надав право регулювання відносин, пов'язаних з набуттям права власності на землю саме Земельному кодексу України.

Згідно із ч. 2 п. 1 ст. 344 ЦК України набуття права власності на земельну ділянку за набувальною давністю регулюється законом. Така позиція, яка серед об'єктів набувальної давності виокремлює землю, є зрозумілою, оскільки йдеться про земельну ділянку як специфічний об'єкт набувальної давності. Звернімо увагу на цивільно-правову побудову статті ЦК стосовно набувальної власності на земельну ділянку. Насамперед з'являється питання, про який закон йдеться у Цивільному кодексі, який буде регулювати набуття права власності на земельну ділянку за набувальною давністю. Очевидно цим положенням зазначено, що регулювання порядку набуття права власності на земельну ділянку за набувальною давністю можливе лише за законом, а не за рішенням уряду чи за іншим підзаконним нормативно-правовим документом.

Верховний Суд України, у Постанові від 3 липня 2018 р. по справі № 670/266/17 констатував: “Набуття права власності на земельну ділянку за набувальною давністю регулюється законом. Апеляційний суд встановив, що спеціальним законом, який регулює порядок набуття права власності на земельну ділянку за набувальною давністю є Земельний кодекс України” [18]. Зазначені обставини істотно впливають на визначення ролі і місця набувальної давності в земельному праві.

Суспільні відносини, що виникають при набутті громадянами права на земельну ділянку за набувальною давністю, регламентуються Земельним кодексом України. Згідно зі ст. 119 Земельного кодексу України громадяни, які добросовісно, відкрито і безперервно користуються земельною ділянкою протягом 15 років, але не мають документів, які б свідчили про наявність у них прав на цю ділянку, можуть

звернутися до органу державної влади або органу місцевого самоврядування з клопотанням про передачу її у власність або надання у користування. Розмір цієї земельної ділянки встановлюється у межах норм, визначених Земельним кодексом України. Передача земельної ділянки у власність або в користування громадянам на підставі набувальної давності здійснюється в порядку, встановленому Земельним кодексом України [1].

Отже, земельне законодавство визначає положення, які регулюють відносини, що виникають у колі набувальної давності, відносно земельних ділянок. Разом з цим відсутні посилання на цивільно-правові норми щодо набувальної давності.

Проаналізуємо та окреслимо особливості застосування набувальної давності по відношенню до земельної ділянки за Цивільним та Земельним кодексами України. Насамперед слід зауважити, що цивільно-правова набувальна давність на майно, як спосіб набуття права власності на нього, відрізняється від набувальної давності у земельному праві, пов'язаної з набуттям земельної ділянки (не тільки у власність, а й окремо у користування), оскільки у Земельному кодексі України йде мова про легалізацію фактичного землекористування, відповідно до визначених умов, передбачених ст. 119 Земельного кодексу України [1].

Разом з тим, втілення положення відносно спроможності одержання громадянами земельної ділянки за набувальною давністю в користування, питання непросте. Право постійного користування земельною ділянкою із земель державної та комунальної власності набувають лише підприємства, установи та організації, що належать до державної або комунальної власності, зазначається у ст. 92 Земельного кодексу України [1]. Враховуючи попереднє положення і те, що суб'єктами набувальної давності в земельному праві можуть виступати тільки громадяни, то безсумнівно, набуття права постійного користування землею за набувальною давністю є фактично нереальним. Громадянам, які мають відношення до набуття за набувальною давністю права орендного (тобто тимчасового та сплатного) землекористування, така можливість за законом не виключається.

Відповідно до ст. 119 Земельного кодексу України коло потенційних суб'єктів набувальної давності на земельну ділянку обмежене тільки громадянами [1]. Тому вони мають можливість реалізувати своє право на набуття земельної ділянки у власність чи орендне землекористування за набувальною давністю у встановленому законом порядку. Відкритим залишається питання щодо можливості розширення кола суб'єктів, які внаслідок набувальної давності можуть набувати земельні права на конкретну земельну ділянку.

Реалізація права, яке належить суб'єктам-громадянам, на набуття земельної ділянки за набувальною давністю здійснюється, враховуючи всі конкретні обставини, за їх волевиявленням. Але потрібно наголосити на тому, що виникнення у суб'єкта права приватної власності на земельну ділянку чи легалізація фактичного землекористування в остаточному результаті залежить від уповноваженого органу державної влади чи органу місцевого самоврядування. У цьому випадку враховується характер цільового використання земельної ділянки та обсяг земельних прав фізичних осіб, залежно від того, чи є конкретна фізична особа громадянином України.

Об'єктом набувальної давності на земельну ділянку може виступати конкретна індивідуально визначена на місцевості земельна ділянка, яка знаходиться у фактичному користуванні громадянина. Межі цієї ділянки склалися в процесі землекористування, яке здійснюється громадянином, і їх ніхто не оспорує: ні суміжні землекористувачі чи власники земельних ділянок, ні треті особи.

Чинне земельне законодавство не встановлює будь-яких обов'язкових вимог щодо цільового використання земельної ділянки – об'єкта, який знаходиться у фактичному (а не юридичному) користуванні громадянина.

Цільове призначення земельної ділянки обов'язково визначатиметься при легалізації фактичного землекористування. Цільове призначення земельної ділянки встановлюється компетентними органами при виникненні земельних прав на цю ділянку за набувальною давністю [14, с. 121-122].

На відміну від ст. 344 ЦК України, в якій йдеться про заволодіння і подальше володіння чужим майном [19], у ст. 119 Земельного кодексу України головною умовою набувальної давності вважається добросовісне, відкрите і безперервне протягом встановленого строку користування земельною ділянкою. Законодавець виділяє у відношенні землі саме давніше користування нею, а не давніше володіння. Це пов'язано з визначенням поняття “користування” у нормах Земельного кодексу України. Право користування землею – це юридично закріплена можливість цільового господарського використання землі та видобування з неї корисних властивостей самим власником земельної ділянки чи уповноваженими ним особами. Зазначене право може бути реалізоване безпосередньо самим власником земельної ділянки. Не виключається можливість, що воно може належати і не власнику, зокрема на підставі адміністративного акту, договору та ін. Це право може здійснюватися, наприклад, постійним землекористувачем, якому в установленому порядку за рішенням уповноваженого органу для певного цільового призначення надана відповідна земельна ділянка, або орендарем на підставі договору оренди. Право користування землею може виникати і на основі прямої вказівки закону, коли йдеться про загальне землекористування (наприклад, у суб'єктів, які використовують землі загального користування в межах населених пунктів). У всіх цих випадках право землекористування не власника виникає і реалізується за волевиявленням власника земельної ділянки [14, с. 122].

У той же час фактичне використання землі суб'єктом – не власником може відбуватись всупереч волі власника конкретної земельної ділянки (наприклад, при самовільному використанні ділянки).

З урахуванням викладених обставин, користування землею можна класифікувати як законне і незаконне. Законне користування землею відбувається на основі чинного законодавства і ним охороняється. Це означає, що має право користування землею. Інші особи можуть користуватися землею, якщо вони отримали дозвіл власника на це.

Межі законного землекористування залежать від цільового призначення відповідної земельної ділянки. Незаконним, з боку землекористувача, є нецільове використання земельної ділянки. Законне користування земельною ділянкою може здійснюватися власником або особами, які мають дозвіл власника на це.

Самовільне використання землі – завжди незаконне. Воно здійснюється як правило не власником або законним землекористувачем. Чинне земельне законодавство щодо самовільного використання землі оперує терміном “самовільне зайняття земельних ділянок”. Такі дії згідно із ст. 211 Земельного кодексу України вважаються земельним правопорушенням, яке становить собою заволодіння земельною ділянкою без законних на те підстав. Воно може виражатися в огороженні земельної ділянки, будівництві на ній певних об'єктів (наприклад, житлового будинку чи нежитлових споруд), проведенні сільськогосподарських робіт, здійсненні іншої діяльності, пов'язаної із фактичним володінням землею [1].

Заволодіння земельною ділянкою без законних підстав є правопорушенням, а суб'єкти, незалежно від того чи користуються землею чи ні, є правопорушниками.

Особа може не користуватися земельною ділянкою, а бути незаконним власником. Фактичне користування земельною ділянкою тісно пов'язане із володінням нею. Вони здійснюються одночасно, але володіння конкретною ділянкою є первинним для користування, хоча право користування землею в окремих випадках може здійснюватись і без права володіння нею [14, с. 124]. Власник земельної ділянки має землю у своєму володінні і сам здійснює фактичне господарювання на ній.

Як право фактичного (фізичного чи господарського) панування на певній земельній ділянці правомочність володіння робить можливим здійснення з боку власника інших правомочностей: користування та розпорядження ділянкою. Право володіння землею може належати не тільки власнику, а й іншим особам. В останньому випадку воно може бути засноване на законі, договорі з власником землі або адміністративному акті. Перебування земельної ділянки на законних підставах у володінні особи обумовлює обов'язковість використання цієї ділянки за цільовим призначенням. Таке володіння землею визнається законним, оскільки воно має певну правову основу (титул). Незаконне володіння вважається без титульним [14, с. 124].

Основними ознаками набувальної давності за ст. 344 ЦК України є:

- володіння є добросовісним, якщо особа при заволодінні чужим майном не знала і не могла знати про відсутність у неї підстав для набуття права власності;
- володіння визнається відкритим, якщо особа не приховувала факт знаходження майна в її володінні. Вжиття звичайних заходів щодо забезпечення охорони майна не свідчить про приховування цього майна;
- володіння визнається безперервним, якщо воно не переривалось протягом всього строку набувальної давності. У разі втрати не із своєї волі майна його давнісним володільцем та повернення цього майна протягом одного року або пред'явлення протягом цього строку позову про його витребування, набувальна давність не переривається (частина третя статті 344 ЦК). Не переривається набувальна давність, якщо особа, яка заявляє про давність володіння, є сингулярним чи універсальним правонаступником, оскільки в цьому разі вона може приєднати до часу свого володіння увесь час, протягом якого цим майном володіла особа, чийм спадкоємцем (правонаступником) вона є (частина друга статті 344 ЦК) [19].

Основною умовою набувальної давності на земельну ділянку є добросовісність. Існує проблема добросовісності фактичного землекористування в сучасній юридичній науці, яка потребує самостійного дослідження. На відміну від фактичного володіння майном у цивільному праві, фактичне земельне користування має негативні наслідки для особи, яка володіє земельною ділянкою добросовісно або недобросовісно.

Добросовісність передбачає, що володілець майна не знав і не міг знати про те, що він володіє чужим майном, тобто ті обставини, які обумовили його володіння, не давали і не могли давати володільцю сумніву щодо правомірності його володіння майном. Цей висновок Верховний Суд зробив у Постанові від 27 вересня 2018 р., по справі № 571/1099/16-ц та Постанові від 31 жовтня 2018 р., по справі № 683/2047/16-ц. [2].

Володіння, що виникло в результаті злочину, не може вважатися добросовісним.

Відкритість володіння означає, що воно є очевидним для усіх третіх осіб, які повинні мати можливість спостерігати за ним, але це не означає, що володілець зобов'язаний спеціально інформувати оточуючих про своє володіння річчю [20].

Відкритим слід вважати таке фактичне землекористування, яке відоме як уповноваженим органам, так і будь-яким іншим особам. У процесі відкритого землекористування суб'єкт здійснює привласнення корисних властивостей земельної ділянки і вважає таке користування правомірним. Підтвердженням відкритого

землекористування може виступати, наприклад, сплата земельного податку за ініціативою громадянина. Доказами відкритого землекористування можуть бути будь-які фактичні обставини, які безперечно підтверджують використання конкретної земельної ділянки громадянином [14, с. 125].

Якщо володіння земельною ділянкою відбувалося безперервно, постійно, з однією і тією ж метою, то воно визначається безперервним.

Володіння визнається безперервним, якщо воно не переривалося протягом всього строку набувальної давності.

Володіння майном повинно бути безперервним протягом установлених законом строків (відповідно до ч. 2 ст. 344 ЦК особа, яка володіє майном, до часу свого фактичного володіння може приєднати час, протягом якого цим майном володіла особа, чийм спадкоємцем (правонаступником) вона є) [9, с. 31].

Користування земельною ділянкою повинно вважатися безперервним і в тому випадку, коли перерва у використанні земельної ділянки пов'язана з характером її використання. Наприклад, безперервним доцільно вважати й таке використання земельної ділянки, коли з урахуванням її цільового характеру експлуатація ділянки можлива через певні проміжки часу (наприклад, виключаючи період промерзання ґрунту та ін.). Безперервне фактичне користування земельною ділянкою повинно бути стабільним, сталим: здійснюватися протягом певного проміжку часу (мінімум 15 років) [21, с. 219].

Прикладом добросовісного, відкритого і безперервного користування земельною ділянкою, яке може бути підставою для набуття права на цю ділянку, є використання службових земельних наділів. Свого часу такі наділи надавалися окремим категоріям працівників у зв'язку з виконанням ними трудової функції на конкретному підприємстві. Але і чинний, і попередній Земельні кодекси України, на жаль, навіть не згадують про службові земельні наділи. Громадяни, які до теперішнього часу користуються службовими земельними наділами, мають право на оформлення фактичного землекористування за давністю користування [21, с. 220].

Отже, умови набуття права власності за давністю користування землею (земельною ділянкою) в деякій мірі узгоджуються з умовами набуття права власності за давністю володіння іншим майном. Однак, наявні й деякі відмінності.

Земельний кодекс України визначає давнісним не володіння, а користування, що пов'язано зі специфікою об'єкту, який набувається за набувальною давністю. В той час як Цивільний кодекс містить поняття добросовісного заволодіння, Земельний кодекс України вказує на добросовісність користування. Адже, добросовісне заволодіння, як зазначалось вище, для Земельного кодексу України неприйнятне.

Відкритість та безперервність для обох кодексів має одне значення й відповідно тлумачиться таким же чином.

Земельний кодекс України коло суб'єктів давнісного користування обмежує тільки громадянами. До того ж він передбачає як закріплення права користування за громадянами так і набуття права власності за давністю користування. Необхідно зазначити, що дане користування здійснюється громадянами, які не мають документів, що засвідчують їх права на дану земельну ділянку.

Порядок передачі у власність чи у користування земельних ділянок визначений відповідно ст. 125 Земельного кодексу України [1].

Висновки.

Інститут набувальної давності згідно Земельного кодексу України потребує деяких до нього уточнень відповідно до норм та узгодження з відповідними нормами ЦК України, зокрема:

- доцільно було б законодавчо удосконалити положення, які існують про набуття прав на земельну ділянку за набувальною давністю шляхом визначення конкретного механізму підтвердження ознак набувальної давності;

- варто було б зменшити строк набувальної давності з 15 років до 10 років.

На наш погляд, можливо, доречним буде використання положень європейського права, зокрема, Кодексу Наполеона, де набуття права власності на землю за давністю володіння, як і в ЦК Російської Федерації, не виокремлюється.

Використана література

1. Земельний кодекс України: Закон України від 25.10.01 р. № 2768-III. URL: <https://www.zakon.rada.gov.ua/laws/show/2768-14>
2. Білий Я.В. Обставини, мають бути доведені при вирішенні спорів, пов'язаних із набуттям права власності за набувальною давністю. URL: <https://www.radako.com.ua/news>
3. Брикайло Ю. Дотримання всіх умов набувальної давності не призводить до виникнення права власності на землю. URL: <http://www.dreamdim.ua/uk>
4. Панченко І.М. Визнання права власності як спосіб захисту цивільних прав: дис. ...канд. юрид. наук: 12.00.03. Київ, 2016. 204 с.
5. Стаценко О.С. Набуття права власності на нерухоме майно за набувальною давністю: дис. ...кандидата юрид. наук: 12.00.03. Одеса, 2019. 224 с.
6. Губарєв С. Право власності фізичної особи на присадибну земельну ділянку (садиби): автореф. дис. ...канд. юрид. наук: 12.00.03. Київ, 2009. 19 с.
7. Мірошніченко А.М., Куцевич О.П. Набуття права власності на нерухоме майно за набувальною давністю в умовах обов'язкової державної реєстрації речових прав. *Наше право*. 2015. № 1. С. 110-114.
8. Ріпенко А.І. Питання захисту речових прав на земельні ділянки в останніх актах судової практики. *Право і громадянське суспільство*. 2013. № 4. URL: <http://www.lcslaw.knu.ua/index.php/arkhiv-nomeriv/4-5-2013/item/134-pytannia-zakhystu-rechovykh-prav-na-zemelni-dilianky-v-ostannikhaktakh-sudovoi-praktyky-ripenko-a-i>
9. Федорченко М.С. Набувальна давність у земельному праві України: науково-практичний коментар. Київ: ІРЦ "Реформування земельних відносин в Україні", 2007. 64 с.
10. Шульга М. Набувальна давність на земельну ділянку: на шляху з минулого у майбутнє. *Вісник Академії правових наук України*. 2002. № 4. С. 16-125.
11. Марусенко Р. Проблеми набуття права власності на землю за набувальною давністю. *Журнал східноєвропейського права*. 2019. № 60. С. 93-105.
12. Дудник К. Проблеми застосування набувальної давності в земельному праві. "ЮРИСТ & ЗАКОН". Аналітичне видання. 2015 № 16(312). URL: <http://www.svitprava.com.ua/uk/korisne/publikatsiji/287-problemi-zastosuvannya-nabuvalnoji-davnosti-v-zemelnomu-pravi.html>
13. Решетник Л.П. Правові проблеми набувальної давності на землю. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія"*. 2014. Вип. 4. С. 161-168.
14. Любич В. Чи можна стати власником землі за набувальною давністю. URL: https://www.protocol.ua/ua/chi_mogna_stati_vlasnikom_zemli_z_nabuvalnoyu_davnistyu
15. Фасій Б.В., Матвійчук А.В. Проблеми застосування інституту набувальної давності за цивільним законодавством України. *Науковий вісник публічного та приватного права*. 2018. Вип. 6. Т. 1. С. 163-167. URL: http://www.nvppp.in.ua/vip/2018/6/tom_1/33.pdf
16. Маковій В.П. Сутність давнісного користування за чинним законодавством: матеріали міжнародної науково-практичної конференції, присвяченій пам'яті професора О.А. Пушкіна, м. Харків, 23 травня 2009 р. Харків: Вид-во Харк. нац. ун-ту внутр. справ. 2009. С. 216-221.
17. Маковій В.П. Набувальна давність у цивільному праві: автореф. дис. ...канд. юрид. наук: 12.00.03. Харків, 2007. 20 с.

18. Черкаська Н.В., Коряченко А.О. Щодо наявності умов набуття земельної ділянки за набувальною давністю громадянами України. *Форум права*. 2013. № 1. С. 1130-1134.

19. Цивільний кодекс України: Закон України від 16.01.03 р. № 435-IV *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356.

20. Постанова Верховного Суду України від 03.07.18 р. по справі № 670/266/17, провадження № 61-7680 св 18.

21. Науково-практичний коментар Цивільного кодексу України; за ред. О.В. Дзери, Н.С. Кузнецової. Київ: Юрінком Інтер, 2006 р. Т. I. С. 566.

~~~~~ \* \* \* ~~~~~

**До відома читачів****РЕКОМЕНДАЦІЇ**

міжнародної науково-практичної конференції на тему:

**“СИСТЕМА ВІЙСЬКОВОЇ ЮСТИЦІЇ  
У ЗАБЕЗПЕЧЕННІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ”,**

м. Київ, 29 жовтня 2019 р.

Міжнародна науково-практична конференція “Система військової юстиції у забезпеченні національної безпеки України”, організована Міністерством оборони України, Секцією права національної безпеки та військового права Національної академії правових наук України та Науково-дослідним інститутом інформатики і права НАПрН України спільно з Військовим інститутом Київського національного університету імені Тараса Шевченка та Військово-юридичним інститутом Національного юридичного університету імені Ярослава Мудрого, була проведена 29 жовтня 2019 року в м. Києві за участі представників Верховної Ради України, суб’єктів сектору безпеки і оборони та інших державних органів, навчальних закладів і наукових установ України, а також представників посольств країн-членів НАТО в Україні.

В ході конференції розглянуто питання щодо захисту конституційних прав і свобод військовослужбовців та членів їх сімей, відновлення системи військової юстиції та її складових, визначення їхніх завдань і функцій, організації досудового розслідування військових злочинів, злочинів проти миру, безпеки людства та міжнародного правопорядку, а також адаптації національної системи військової юстиції до стандартів країн-членів НАТО.

Учасники конференції *констатували*:

– Україна має багатовіковий досвід державотворення, військового будівництва і забезпечення правопорядку у воєнній сфері, починаючи з часів Київської Русі, Козацької держави Богдана Хмельницького, Української Народної Республіки та інших державних утворень;

– у 1990-х роках з набуттям незалежності в Україні було сформовано розгорнуту систему військової юстиції, що включала: *військові суди регіонів і гарнізонів; військові прокуратури регіонів та гарнізонів; юридичні підрозділи військових формувань; військово-юридичні навчальні підрозділи у складі Київського національного університету імені Тараса Шевченка та Національного юридичного університету імені Ярослава Мудрого*. Крім цього, було запроваджено навчальну і наукову спеціальність “Військове право”;

– протягом 2001 – 2011 років в умовах безсистемного скорочення військових формувань (*їх чисельність у 1991 р. становила понад 1 млн. 100 тис. чоловік*), розпродажу військових об’єктів, техніки і майна, система військової юстиції була повністю ліквідована. Зазначене, як засвідчили події 2014 – 2015 рр. у воєнній сфері, призвело до негативних процесів у забезпеченні правопорядку та підтриманні обороноздатності держави;

– в сучасних умовах гібридної війни, міжнародного військового конфлікту, проведення антитерористичної операції та операції об'єднаних сил, анексії РФ Автономної республіки Крим та окупації окремих районів Донецької і Луганської областей нагальною постає проблема відновлення і розвитку системи військової юстиції в Україні.

З урахуванням зазначеного та результатів всебічного обговорення піднятих питань конференція *рекомендує*:

1. Звернутися до Президента України, Верховної Ради України, Кабінету Міністрів України та Верховного суду України з пропозиціями щодо відновлення і розвитку системи військової юстиції з урахуванням історичного досвіду України і стандартів кран-членів НАТО щодо захисту конституційних прав військовослужбовців і членів їх сімей та підтримання правопорядку у воєнній сфері.

2. Віднести згідно з положеннями Конституції України та чинного законодавства до основних складових національної системи військової юстиції: *спеціалізовані військові суди; спеціалізовану прокуратуру у воєнній сфері; державний правоохоронний орган зі спеціальним статусом у воєнній сфері (Державна служба військової юстиції, Військова поліція); юридичні підрозділи військових формувань; військово-юридичні навчальні підрозділи у складі Київського національного університету імені Тараса Шевченка та Національного юридичного університету імені Ярослава Мудрого, а також відновлену 2018 року наукову і навчальну спеціалізацію “Право національної безпеки та військове право”.*

3. Сформувати державний правоохоронний орган зі спеціальним статусом у воєнній сфері шляхом реорганізації Військової служби правопорядку Збройних Сил України та за рахунок скорочених підрозділів і військовослужбовців органів військової прокуратури з метою збереження кадрового потенціалу і зменшення бюджетних витрат. Діяльність вказаного органу, з урахуванням досвіду реформування МВС України, може спрямовуватися і координуватися через Міністра оборони України.

4. До завдань державного правоохоронного органу зі спеціальним статусом у воєнній сфері рекомендується віднести:

1) захист прав, свобод і законних інтересів військовослужбовців, резервістів та військовозобов'язаних під час проходження ними зборів, а також членів їхніх сімей;

2) забезпечення правопорядку у Збройних Силах України та інших військових формуваннях, створених відповідно до законодавства України;

3) попередження, виявлення і припинення правопорушень, протидія кримінальним правопорушенням та корупції у Збройних Силах та інших військових формуваннях, створених відповідно до законодавства України, а також в оборонно-промисловому комплексі держави;

4) здійснення досудових розслідувань у кримінальних провадженнях про кримінальні правопорушення відповідно до визначеної підслідності;

5) участь у забезпеченні правопорядку в районах бойових дій, зонах проведення операцій об'єднаних сил, миротворчих і антитерористичних операцій та у протидії диверсіям і терористичним актам на військових об'єктах;

б) забезпечення виконання кримінальних і адміністративних покарань (у дисциплінарному батальйоні та на гауптвахті) відповідно до законодавства та участь в охороні військових об'єктів, визначених Кабінетом Міністрів України.

5. Національному університету оборони України імені Івана Черняхівського, Військовому інституту Київського національного університету імені Тараса Шевченка, Військово-юридичному інституту Національного юридичного університету імені Ярослава Мудрого та іншим закладам вищої освіти сектору безпеки і оборони за сприяння Секції права національної безпеки та військового права Національної академії правових наук України і Науково-дослідного інституту інформатики і права НАПрН України забезпечити розробку і впровадження у навчальний процес і наукову діяльність нових спеціалізацій з питань права національної безпеки та військового права.

6. Міністерству оборони України спільно з Національною академією правових наук України (*Секцією права національної безпеки та військового права НАПрН України і Науково-дослідним інститутом інформатики і права НАПрН України*) у взаємодії з Комітетом Верховної Ради України з питань національної безпеки, оборони і розвідки забезпечити підготовку проектів законів України, спрямованих на реалізацію вказаних рекомендацій.

URL: [//www.ippi.org.ua](http://www.ippi.org.ua)

~~~~~ \* \* \* ~~~~~

РЕКОМЕНДАЦІЇ

міжвідомчого “круглого столу” на тему:

“НАУКОВА ДІЯЛЬНІСТЬ ТА ІНФОРМАЦІЯ З ОБМЕЖЕНИМ ДОСТУПОМ: АКТУАЛЬНІ ПРОБЛЕМИ І ШЛЯХИ ЇХ ВИРІШЕННЯ”,

м. Київ, 14 листопада 2019 року

Згідно з ініціативою суб'єктів сектору безпеки і оборони України 14 листопада 2019 року в Національній академії Служби безпеки України відбувся міжвідомчий “круглий стіл” – “Наукова діяльність та інформація з обмеженим доступом: актуальні проблеми і шляхи їх вирішення” за участі представників Комітету Верховної Ради України з питань освіти, науки та інновацій, Міністерства освіти і науки України, Національного агентства з питань оцінювання якості вищої освіти, Міністерства оборони України, Міністерства внутрішніх справ України, Служби безпеки України, Державної прикордонної служби України, Національної гвардії України, Державної служби з надзвичайних ситуацій, розвідувальних органів України, Національної академії наук України, Секції права національної безпеки та військового права Національної академії правових наук України, вищих навчальних закладів і наукових установ суб'єктів сектору безпеки і оборони України. В ході “круглого столу” було розглянуто комплекс актуальних проблем щодо організації та здійснення наукової, науково-технічної і науково-педагогічної діяльності у сфері національної безпеки і оборони, використання інформації з обмеженим доступом, захисту національних інтересів у сфері освіти і науки та конституційних прав вчених.

Учасники “круглого столу” *констатували*:

– останніми роками прийнято низку нормативно-правових актів, які ставлять у пряму залежність вирішення питань захисту дисертацій доктора філософії і доктора наук, присудження наукових ступенів, присвоєння вчених звань, формування редакційних колегій наукових фахових видань та разових спеціалізованих вчених рад від наявності опублікованих статей у періодичних виданнях, включених до наукометричних баз Scopus або Web of Science Core Collection (виданнях категорії А, що мають статус іноземних юридичних осіб та є комерційними організаціями створеними з метою отримання прибутку). Зазначене містить ознаки порушення антикорупційного і антимонопольного законодавства, призводить до порушення конституційних прав вчених та створює реальні передумови до витоку відомостей щодо результатів досліджень, які можуть містити державну, комерційну таємницю або іншу інформацію з обмеженим доступом;

– аналіз зарубіжного досвіду свідчить, що наявність чи відсутність вказаних публікацій є лише формальним показником, який має інформаційне значення і не повинен мати нормативного характеру. Згідно з оцінкою найбільш авторитетних академій наук Європейського Союзу (Академії наук Франції, Німецької академії природничих наук (“Леопольдіна”), Королівської академії наук Великої Британії), наявність публікацій у журналах, включених до наукометричних баз, не може розглядатися як один із основних інструментів оцінювання результатів наукових досліджень, а покладання на цей показник “веде до поверхових, занадто спрощених і ненадійних методів оцінювання”. Польські вчені також аргументовано доводять, що багатовимірною оцінкою місцевих журналів не повинна спиратися лише на бібліометричні показники, засновані на Web of Science або Scopus;

– наукові дослідження з проблем національної безпеки і оборони мають надзвичайно важливе значення в умовах гібридної війни та євроатлантичної інтеграції України, а оприлюднення їх результатів має відбуватися з дотриманням необхідних вимог у сфері охорони державної таємниці та інших відомостей з обмеженим доступом. Положення нормативно-правових актів з питань освіти і науки також мають відповідати вимогам закону у цій сфері та не спричиняти передумов до витоку наукової інформації з обмеженим доступом щодо напрямів, наукових ідей, науково-технічних розробок та їх авторів до спецслужб іноземних держав і не сприяти відтоку наукових кадрів;

– низка галузей науки, зокрема соціогуманітарних, які забезпечують розвиток Української державності, правосвідомості, національної культури і мистецтв, як правило, не представляють інтересу для наукометричних баз Scopus або Web of Science Core Collection, однак використання інших міжнародних і національних наукометричних баз чинне законодавство з питань освіти і науки не передбачає;

– актуальним є формування Українського національного індексу цитування (УНІЦ), визнаного міжнародними наукометричними системами, що сприятиме підвищенню оцінки реальних наукових надбань українських вчених під час державної атестацій наукових установ та наукових співробітників, у тому числі які працюють з інформацією з обмеженим доступом.

За результатами обговорення винесених на розгляд актуальних проблем учасники “круглого столу” **рекомендують**:

1) створити робочу групу за участі представників Президії і наукових установ Національної академії наук України (Національної бібліотеки України ім. В.І. Вернадського, Інституту програмних систем, Інститут досліджень науково-технічного потенціалу та історії науки імені Г.М. Доброва, Інституту проблем реєстрації інформації, Українського мовно-інформаційного фонду, Центру досліджень інтелектуальної власності та трансферу технологій), Національної академії правових наук України (Науково-дослідного інституту інформатики і права, Науково-дослідного інституту інтелектуальної власності, Секції права національної безпеки та військового права), Українського інституту науково-технічної експертизи та інформації, Державної науково-технічної бібліотеки, Служби безпеки України, Міністерства оборони України, Міністерства освіти і науки України, а також навчальних закладів і наукових установ, які працюють з інформацією з обмеженим доступом, для розроблення пропозицій щодо:

– унормування порядку присвоєння вчених звань і створення спеціалізованих вчених рад, присудження наукових ступенів доктора філософії та доктора наук за результатами прилюдного захисту дисертацій, що мають гриф секретності (“цілком таємно”, “таємно”, “для службового користування”) згідно з вимогами Закону України “Про державну таємницю”;

– розробки і затвердження Порядку формування Переліку наукових фахових видань України, в яких мають публікуватися результати наукових і науково-технічних досліджень та розробок вчених, що містять інформацію з обмеженим доступом;

– розвитку Українського національного індексу цитування, обов’язкового для відкритих видань, а також для публікацій, що містять інформацію з обмеженим доступом, з окремим порядком їх аналізу, утворення технічної служби УНІЦ, яка займатиметься питаннями забезпечення її роботи та організації діяльності вказаної служби;

2) підтримати пропозиції, викладені у рішенні Комітету Верховної Ради України з питань освіти, науки та інновацій від 6 листопада 2019 року про створення національної наукометричної бази наукових періодичних видань та опрацювати питання щодо можливого включення до неї сегменту з матеріалами з обмеженим доступом;

3) рекомендувати МОН України забезпечити приведення нормативно-правових актів з питань освіти і науки до потреб захисту конституційних прав вчених, національних інтересів і національної безпеки, зокрема, внесення змін і доповнень до таких правових актів:

– до п. 1 наказу МОН України “Про затвердження Порядку формування Переліку наукових фахових видань України” від 15 січня 2018 року № 32, виклавши його у такій редакції: “1. Затвердити Порядок формування Переліку наукових фахових видань України, що додається. Положення Порядку формування Переліку наукових фахових видань України не поширюються на видання, що мають гриф обмеження доступу”;

– до постанов Кабінету Міністрів України та наказів МОН України з питань наукової, науково-технічної і науково-педагогічної діяльності в яких слова “Scopus” та “Web of Science” замінити словами “у міжнародних і національних наукометричних базах”;

4) науковим установам і навчальним закладам, які є суб’єктами діяльності, пов’язаної з обігом інформації з обмеженим доступом, забезпечити належну роботу комісій з питань таємниць, що мають визначати наявність чи відсутності інформації з обмеженим доступом у наукових роботах, поданих до опублікування;

5) направити рекомендації “круглого столу” “Наукова діяльність та інформація з обмеженим доступом: актуальні проблеми і шляхи їх вирішення” Президенту України, Голові Верховної Ради України, Прем’єр-міністру України, Секретарю Ради національної безпеки і оборони України, до Комітету Верховної Ради з питань освіти, науки та інновацій, а також Міністерства освіти і науки України.

URL: [//www.ippi.org.ua](http://www.ippi.org.ua)

~~~~~ \* \* \* ~~~~~

## РЕЦЕНЗІЯ

на монографію **“Національна безпека України в інформаційну епоху: правові аспекти”** / авт. І.М. Доронін

Складний характер сучасного інформаційного суспільства зумовлює необхідність проведення наукових досліджень щодо суті та трансформацій суспільних інститутів, до числа яких належить держава, і відповідних регуляторів суспільних відносин. За таких умов потребує уточнень також і традиційне сприйняття феномену “національної безпеки”. Останнім часом актуалізація проблематики досліджень у сфері національної безпеки відбулась внаслідок низки трагічних для суспільства подій, що підняло на порядок денний питання ефективності існуючого механізму держави в контексті нейтралізації та подолання викликів і загроз. Попередні напрацювання науковців у сфері національної безпеки та оборони стосувались періоду становлення української державності відразу після розпаду Радянського Союзу, який характеризувався існуванням дещо інших викликів та загроз.

Реагування на актуальні виклики і загрози зумовили і значне оновлення чинного законодавства у сфері національної безпеки і оборони України, що не позбавлено ознак безсистемності та певної хаотичності. До того ж складна внутрішньополітична ситуація в державі здійснювала і здійснює свій негативний вплив на прийняття законодавчих актів. Такий стан речей може бути проілюстровано постійним оновленням законодавчої бази, прийняттям та скасуванням окремих законодавчих актів, звичним вже уточненням аргументації законодавців щодо необхідності правової регламентації тих чи інших суспільних відносин. Слід додати також і фактор відсутності визначеної ідеології у модернізації вітчизняної правової системи.

Обрана автором тема для дослідження – зміна феномену “національної безпеки” у сучасному світі, а також його сприйняття і відображення у праві, є цікавою та актуальною для сучасної правової науки. Як вбачається із структури роботи, автор досліджує проблематику національної безпеки України у різних аспектах – на рівні визначення поняття та його суті (концепту), у розрізі трансформації сприйняття феномену в суспільній думці та гуманітарних науках, через призму правового регулювання відповідних суспільних відносин, а також в його історико-правовому розвитку.

У монографії пролунало нове звучання концепції виокремлення основної (генеральної) функції держави, зміст якої автором запропоновано розглядати як забезпечення національної безпеки. За таких умов інші функції держави визначаються враховуючи їх суть, що полягає у забезпеченні безпеки. Новою авторською ідеєю є сприйняття системи державних функцій саме у контексті забезпечення безпеки. Цікавим є також обрання змісту функції як обґрунтування мети і меж втручання держави у суспільні відносини. Така авторська точка зору, безумовно, є дискусійною і потребуватиме додаткової аргументації у подальших роботах.

Слід також звернути увагу і на виокремлення автором періоду “інформаційної епохи”, як своєрідних хронологічних рамок дослідження. Авторська позиція з цього приводу полягає у визначенні певного періоду розвитку людства, що характеризується широким застосуванням технології переробки, розповсюдження та зберігання інформації. Підґрунтям для такої точки зору є відповідні дослідження соціології аналіз яких наведено у роботі. Слід зауважити, що з точки зору соціальної філософії питання

періодизації розвитку людства є доволі складним і багатограним. Водночас, таке окреслення хронологічних рамок для роботи дозволило дослідити і висвітлити певні феномени, що притаманні саме інформаційному суспільству.

Проблеми правової регламентації, які виникають у сфері національної безпеки, адекватним чином визначено у відповідних главах роботи, що присвячені становленню та розвитку специфічних підгалузей законодавства, яке започатковано та виникло в умовах протидії агресії. Насамперед мова йде про дослідження проблем застосування державою санкцій поза межами юридичної відповідальності з метою забезпечення національної безпеки, встановлення певних правових обмежень, а також особливостей у застосуванні правових приписів. Цікавим є проведений аналіз практики застосування законодавства у сфері національної безпеки в контексті визначення державних інтересів (“інтересів національної безпеки”), як підстави для тимчасового обмеження окремих прав і свобод людини і громадянина.

У питанні перспективного правового регулювання варто звернути увагу на складний характер наукової проблеми можливого виокремлення права національної безпеки в умовах сучасної систематизації права. Зазначені питання також розглянуто автором, наведено певну аргументацію на підтримку точки зору стосовно виокремлення права національної безпеки. Разом із цим, слід зазначити, що питання визначення предмету та особливо методу, як підстави розподілу права на відповідні галузі, є складними і потребуватимуть подальшого ґрунтовного висвітлення. До того ж неодмінно виникатиме питання і у необхідності визначення системи для нової галузі, а також можливості існування певних комплексних правових інститутів.

Слід підтримати зусилля автора, спрямовані на дослідження проблем правової регламентації в сучасному глобалізованому світі в контексті інформаційних відносин та регулювання розповсюдження новітніх технологій з точки зору забезпечення національної безпеки України.

Таким чином, монографія І.М. Дороніна “Національна безпека України в інформаційну епоху: правові аспекти” є комплексною науковою працею, що виконана на актуальну тему, вона має наукову й практичну цінність. Результати дослідження, наведені у монографії, можуть бути використані у навчальному процесі, зокрема при викладанні курсів “теорія держави і права”, “національна безпека України”, а також у наукових дослідженнях з проблем теорії та історії держави і права, національної безпеки та державного управління.

Керівник науково-дослідного центру правового  
забезпечення інформаційної і національної  
безпеки НДПП НАПрН України,  
заслужений юрист України,  
доктор юридичних наук, професор

Є.Д. Скулиш

~~~~~ \* \* \* ~~~~~

До відома авторів

“ІНФОРМАЦІЯ І ПРАВО” – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямками досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:

- у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;
- параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;
- відстань між рядками – 1 інтервал;
- кількість матеріалу однієї статті – не більше 15 стор.

Стаття має передбачати такі обов’язкові структурні елементи:

- УДК.
- Ім’я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.
- Назва статті (укр. та англ. мовами).
- Анотація та ключові слова (укр., англ. та рос. мовами).
- Розв’язання проблеми, шляхом наукового вирішення завдання:
 - постановка проблеми (загальна характеристика);
 - результати аналізу наукових публікацій – надаються відомості про стан вирішення проблеми та ПШБ авторів, з обов’язковим посиланням на їхні роботи (в [...]), повний опис бібліографії яких вказується в підрозділі “Використана література”; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;
 - формування мети (постановка завдання) статті;
 - виклад основного матеріалу – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
- Висновки за результатами розв’язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
- Використана література. Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 “Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання” або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.
- Підпис, адреса (е-адреса), телефон автора.

2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- *Актуальність теми.*
- *Новизна та обґрунтованість одержаних результатів.*
- *Наукова (практична) цінність результатів.*
- *Висновок про можливість відкритої публікації.*

3) Рукопис статті та Відгук мають бути ретельно вчитаними, виправленими і підписаними відповідними особами.**4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України “Про затвердження порядку формування переліку наукових фахових видань України” від 17.10.12 р. № 1111.****5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту.**

Реквізити для оплати робіт:

Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада НДПП НАПрН України не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції. Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за дотримання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:
 - відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
 - внесення до статті змін редакційного змісту у зв’язку з обмеженням обсягу загального матеріалу.

*** * * * ***

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(32)/2020

| | |
|---|--|
| Засновники журналу: | <ul style="list-style-type: none"> - Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІП НАПрН України); - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини “Україна”. |
| Видавець: | © НДІП НАПрН України. |
| Адреса редакції: | 01032, м. Київ, вул. Саксаганського, 110-В.
Науково-дослідний інститут інформатики і права
Національної академії правових наук України.
Тел.: 234-94-56; e-mail: bvm777@ ukr.net |
| Веб-сторінки журналу у мережі Інтернет: | URL: //www.ippi.org.ua – НДІП НАПрН України;
URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського. |
| Founders of journal: | <ul style="list-style-type: none"> - Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine (SRIIL of the NALS of Ukraine); - Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine; - Open International University of Human Development “Ukraine” |
| Publisher: | © SRIIL of the NALS of Ukraine. |
| Address of release: | 01032, Kyiv, Saksaganskogo str., 110-V.
Scientific Rresearch Institute of Informatics and Law
of the National Academy of Law Sciences of Ukraine.
Phone: 234-94-56; e-mail: bvm777@ ukr.net |
| Web-pages of journal in the network Internet: | URL: //www.ippi.org.ua – Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine;
URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine. |