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

№ 4(31)/2019

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

№ 4(31)/2019

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.

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

До відома читачів

Нове наукове видання:

Інформаційне право та інформаційне законодавство: наукове видання / Брижко В.М., Фурашев В.М. – (Рекомендовано до друку Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України, протокол № 7 від 30.10.2019 р.), Київ: Видавничий дім "АртЕК", 2020. 288 с……..... **129**

Рецензія на монографію:

"Публічне адміністрування національно-безпековою сферою в Україні: теоретико-правові та організаційні засади" / автор К.В. Бондаренко; рецензент професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права, психології та інноваційної освіти Національного університету "Львівська політехніка", доктор юридичних наук, професор Л. Чистоклетов…….……..... **131**

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Граматичне коректування – Майстренко І.А. (укр., англ.).

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 12.1. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ "Видавничий дім "АртЕк".
04050, м. Київ, вул. Мельникова, буд. 63. Свідоцтво 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 НДІІП НАПрН України, протокол № 10 від 24.12.19 р.

T A B L E O F C O N T E N T S

Informative Law

Legal Informatics

Informative and National Safety

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

For the consideration of readers

New Scientific Edition:

Review of the monograph:

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 10 dated 24.12.19

Інформаційне право

УДК 316(477)

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,*
головний науковий співробітник НДІІП НАПрН України
РУБАН О.О., *кандидат юридичних наук*, асистент кафедри цивільного права № 2
Національного юридичного університету імені Ярослава Мудрого

ВІДПОВІДАЛЬНІСТЬ: ДО ПРОБЛЕМИ КОНЦЕПТУАЛІЗАЦІЇ КАТЕГОРІЇ

Анотація. *У статті феномен відповідальності розглядається як соціально-історичне явище, яке з'являється як результат виникнення й розвитку суспільних відносин і як характеристика відносин між особистістю, соціальною групою і суспільством у цілому. Проаналізовані ключові концептуальні підходи до розуміння відповідальності в історії розвитку філософської культури. Робиться висновок, що основною тенденцією в інформаційному суспільстві стає повсюдний відхід від відповідальності фактично на всіх рівнях її прояву, що дозволяє вести мову про асиметричність розвитку суспільства: надзвичайно високий ступінь технологічного розвитку супроводжується деградацією етики й моралі. Це стає основною суперечністю, що продукує соціальні конфлікти від міжособистісних до міждержавних.*

Ключові слова: *відповідальність, свобода, обов'язок, соціальна активність, спосіб життя.*

Summary. *In the article the phenomenon of responsibility is considered as a socio-historical phenomenon that appears as a result of the emergence and development of social relations and as a characteristic of relations between the individual, social group and society as a whole. The key conceptual approaches to the understanding of responsibility in the history of the development of philosophical culture are analyzed. It is concluded that a major trend in information society is ubiquitous abdication of responsibility at virtually every level of its manifestation, which allows to talk about the asymmetry of society development : the extremely high degree of technological development is accompanied by the degradation of ethics and morality. This becomes the primary contradiction, that generates social conflicts, from interpersonal to international.*

Keywords: *responsibility, freedom, duty, social engagement, life style.*

Аннотация. *В статье феномен ответственности рассматривается как социально-историческое явление, возникающее как результат возникновения и развития общественных отношений и как характеристика отношений между личностью, социальной группой и обществом в целом. Проанализированы ключевые концептуальные подходы к пониманию ответственности в истории развития философской культуры. Делается вывод, что основной тенденцией в информационном обществе становится повсеместный уход от ответственности фактически на всех уровнях ее проявления, что позволяет вести речь об асимметричности развития общества: чрезвычайно высокая степень технологического развития сопровождается деградацией этики и морали. Это становится основным противоречием, продуцирующим социальные конфликты от межличностных до межгосударственных.*

Ключевые слова: *ответственность, свобода, долг, социальная активность, образ жизни.*

Постановка проблеми. На сучасному етапі переходу людства на нову стадію розвитку – від індустріального до інформаційного, процесу інформатизації українського суспільства в умовах глобалізації міжнародних відносин актуалізується роль і значення відповідальності за правопорушення в інформаційній сфері, яка здійснює функцію

регуляції поведінки індивіда відповідно до вимог суспільства. На часі відповідальність набуває провідної ролі в політичних, духовно-ідеологічних та інших відносинах, у тому числі інформаційних, її удосконалення є необхідною умовою суспільного розвитку.

Людство на сучасному етапі розвитку проголосило однією з найважливіших цінностей свободу, яка передбачає, зокрема, подолання залежності не тільки від природи, але й часто від держави, моралі і навіть від соціуму, який визначає цінності і норми поведінки. Таке відчуження людини від суспільства неминуче призводить до атомізації соціуму, а потім, можливо, і до його розпаду, у зв'язку з тим, що суспільство здатне існувати лише за умови наявності у окремих індивідів і в різних соціальних груп солідарних цілей, очікувань і потреб, на сторожі яких стоїть взаємна відповідальність.

Володіючи набагато більшими технічними можливостями та знаннями, аніж це було можливо в усі попередні епохи, наш світ не тільки не позбувся проблем, але й помітно збільшив їх кількість. Людство досягло такої технічної могутності, яка може поставити під загрозу існування як самого людського роду, так і всієї планети. В умовах таких ніким і нічим не обмежених загроз і можливостей лише відповідальність як наріжний принцип побудови соціальних відносин може стати тим вирішальним фактором, який дозволить суспільству не тільки розвиватися, але й просто бути, існувати. Таким чином, сьогодні, у принципово нових умовах існування суспільства, роль і значення відповідальності повинні бути переосмислені і переоцінені, а сама ця проблема повинна зайняти центральне місце в сучасному соціогуманітарному знанні.

Філософами, культурологами, соціологами, політологами, економістами зазначається факт дестабілізації соціальних систем на різних рівнях у масштабі планети, що проявляється у певному занепаді ролі національних держав і національних культур, у кризі індивідуальної, етнічної, громадянської ідентичності, атомізації суспільства, в нестабільності ціннісних систем тощо, що, на нашу думку, також доводить необхідність дослідження проблеми відповідальності у сучасному світі. Глобальні зміни, що відбуваються, призвели до появи абсолютно нових соціокультурних реалій, які володіють негативним "розхитуючим" потенціалом. Серед них – глобалізація, у тому числі глобалізація культури, індивідуалізація суспільства, перетворення масової культури на домінуючу культурну форму, розвиток цінностей суспільства споживання, поширення екранної віртуальної культури тощо [1]. Сучасний етап розвитку характеризується також руйнуванням культурних традицій, девальвацією національних ціннісних систем і побудовою нових на базі цінностей західного світу, а також глобальною кризою відповідальності [2].

Результати аналізу наукових публікацій свідчать про те, що проблемі відповідальності присвячено велику кількість наукових доробків, у яких достатньо ґрунтовно досліджується сутність і особливості вказаного феномена здебільшого у юридичному аспекті. Разом з тим, комплексному філософському розумінню відповідальності у наявних наукових публікаціях приділяється недостатня увага.

Метою статті є спроба уточнити концептуальні моменти проблеми відповідальності в історико-філософському аспекті.

Виклад основного матеріалу. Сучасне суспільство перебуває на такому етапі розвитку, коли процеси, які відбуваються в культурі, економіці, політиці та інших сферах, носять глобальний характер, а рішення, що приймаються на одному континенті, неминуче провокують відгук і трансформацію на іншому. Світ характеризується максимальним ступенем взаємозалежності всіх елементів, чи то держав, економік, соціальних груп, чи то окремих осіб. Людство досягло найвищого рівня технологічного розвитку, який дозволяє не тільки змінити зовнішній вигляд світу за лічені години, а й

знищити саму планету. Такі нічим і ніким необмежені за фактом можливості, вимагають переглянути існуюче ставлення до категорії відповідальності, оскільки лише відповідальність здатна стати тим принципом існування суспільства, який забезпечить безпеку і сталий розвиток як окремих його членів, так і суспільства у цілому.

Феномен відповідальності – явище соціально-історичне, яке з'являється як результат виникнення й розвитку суспільних відносин і як характеристика відносин між особистістю, соціальною групою і суспільством у цілому. З одного боку, суспільство як система продукує комплекс норм, цінностей, вимог, об'єднаних в єдину систему, а з іншого – особистість зобов'язана сприйняти, засвоїти і згодом відтворити ці норми й цінності. Тобто, відповідальність передбачає співвіднесення поведінки особистості (соціальної групи) з відповідністю вимогам, що пред'являються суспільством. Таким чином, відповідальність як соціокультурне явище зароджується разом з суспільством, а як філософська категорія і категорія культури відповідальність з'являється набагато пізніше.

Філософське осмислення сутності відповідальності почалося ще античними філософами. Глибоке і всебічне висвітлення проблема відповідальності отримала в етиці Аристотеля, який досліджував об'єктивні й суб'єктивні передумови відповідальності, зумовлені прагненням людей до загального блага й чесноти. Джерело дій людини знаходиться в ній самій. Згідно з точкою зору Аристотеля, розум і совість в душі у людини дозволяють їй здійснювати "справедливі" вчинки і нести відповідальність за них, тобто бути розсудливою; розсудлива людина прагне до справедливості – міри в різних своїх прагненнях і бажаннях. При цьому, людина чинить неправосудне або правосудне тільки тоді, коли здійснює вчинки по своїй волі, якщо ж має місце насильство, то людина не може нести відповідальність за свої дії. Філософ виходить насамперед із моральної відповідальності людини перед суспільством і державою; її совість, "правосудність" і чеснота мають моральний характер і можуть бути вихована за допомогою розумних і справедливих законів: "Може бути, тому, хто бажає робити людей – багатьох чи небагатьох – кращими, приділяючи увагу їх вихованню, треба постаратися навчитися створювати закони, якщо завдяки законам ми можемо стати добрими" [3, с. 291]. Аристотель, не використовуючи саме поняття відповідальності, описував зв'язок між свободою волі і вибору з необхідністю відповідати за цей вибір. Кожна людина, з точки зору Аристотеля, сама вибирає, як їй вчиняти – добре чи ганебно – і відповідно до зробленого вибору, людину вихваляють або карають. Цікавим є той факт, що незнання за Аристотелем, не є причиною, за якою людину можна звільнити від необхідності відповідати за свій вибір, а навіть навпаки, в деяких випадках лише посилює її провину.

Аналогічні підходи до розуміння відповідальності можна простежити і в точках зору Цицерона, Епікура та інших античних мислителів.

Таким чином, як стверджує І. Осипов, відповідальність в античній культурі може бути визначена як соціально-політична відповідальність розумного громадянина. Суб'єктивний же контекст відповідальності відступає на другий план і багато в чому опосередковується природним розумом, мораллю і правом. Цей стан моральної свідомості І. Осипов називає колективним "моральним інтелектуалізмом" [4, с. 54].

Принципово нова парадигма відповідальності з'являється в епоху Середньовіччя. "З появою християнства акцент повністю переміщається з турботи про світ і пов'язаних з цим обов'язків на турботу про душу і її порятунок. У перші століття полярність цих двох підходів носила абсолютний характер: новозавітні послання сповнені закликів

уникати публічності й політики, займатися своєю, суто приватною справою, піклуватися про власну душу" [5, с. 211].

Відповідальність в епоху Середньовіччя виходить із принципу свободи волі віруючої людини (Августин Блаженний, Фома Аквінський) [6]. Зазначене уявлення гранично суб'єктивує відповідальність і переносить її у "внутрішню людину" (Тертулліан), дозволяє виробити механізм самоцензури на основі почуття страху Божого й совісті. Зі свого боку і Церква на основі канонічного права контролює поведінку прихожанина.

Продовження цілісного осмислення відповідальності як філософської категорії відбувається лише в XVII-XVIII ст. представниками західноєвропейської філософської думки (Т. Гоббс, Дж. Локк). Так само, як і за часів Аристотеля, ними не вживається термін "відповідальність", але описується, по суті, одна з її граней. У раціоналістичній філософії Нового часу народжується нова парадигма відповідальності, яка може бути названа цивільно-правовою відповідальністю особистості (І. Осипов) [4, с. 56]. В цей час збігаються два соціокультурних процеси: народження емансипованої, розумної й відповідальної у правовому відношенні особистості і становлення правової держави. В рамках секуляризації на перший план виходить значення віруючого розуму, який і формує концепт відповідальності, що отримав теоретичне вираження у філософії суспільного договору Т. Гоббса та Дж. Локка.

Так, Т. Гоббс міркував про необхідність громадянам дотримуватися законів і відповідати за їх недотримання та для практичного забезпечення цього обрати суверена. "…Для встановлення загальної влади необхідно, щоб люди призначили одну людину або групу людей, які виявилися б їхніми представниками: щоб кожна людина вважала себе довірителем щодо всього, що носій загальної особи буде робити сам або змусить робити інших відносно загального миру й безпеки, і визнає себе відповідальним за це; щоб кожний підкорив свою волю й судження волі й судженню носія загальної особи" [7, с. 119]. Він дає наступне визначення сутності держави, яке вже враховує категорію "відповідальність": "…Держава є єдиною особою, відповідальною за дії якої зробила себе шляхом взаємного договору між собою величезна кількість людей, для того, щоб ця особа могла використати чинність і кошти всіх їх так, як визнає за необхідне для їхнього миру й загального захисту" [7, с. 119].

Дж. Локк вперше пов'язав відповідальність зі свободою, побачивши, що є щось, що обмежує безумовну свободу людини.

Кульмінаційним пунктом розвитку концепції цивільно-правової відповідальності є вчення І. Канта, який створив власну етику, основою якої стало поняття категоричного імперативу й обов'язку. Категоричний імператив – обов'язковий моральний закон, на який повинні орієнтуватися всі люди, незалежно від статусу, матеріального благополуччя. Обов'язок за І. Кантом – це примушення з боку морального закону вільної волі людини. Моральний закон у даному випадку не є породженням суспільства, а таким собі еталоном поведінки людини. І людина дотримується його лише, з одного боку, через тиск цього закону, а, з іншого – завдяки особистому обов'язку.

"Обов'язок" – категорія безпосередньо пов'язана з відповідальністю, хоча й має істотну відмінність від останньої. Обов'язок завжди має на увазі добровільне покладання особистістю на себе обов'язків. Обов'язок базується на внутрішньому спонуканні діяти у відповідності з моральними переконаннями. Головною інстанцією, яка контролює виконання обов'язку, стає совість, а гарантом – високий духовний рівень людини. Таким чином, за виконання чи невиконання обов'язку людина відповідає лише перед собою і своєю совістю. Відповідальність же буває як добровільною, так і набутою.

Людина може добровільно покласти на себе будь-яку відповідальність за що-небудь, у цьому буде схожість з обов'язком. Але відповідальність може бути покладена на людину або набуватися нею в силу зміни статусу. Наприклад, з народженням дитини батьки відповідають за її долю, при вступі на посаду людина несе відповідальність за виконання посадових обов'язків і т.д. За виконання своїх обов'язків людина відповідає не тільки перед собою, а й перед суспільством. При цьому І. Кант, розмірковуючи про обов'язок, по суті, описував найвищу ступінь відповідальності – етичну відповідальність, де орієнтиром виступають не існуючі норми моралі, а ідеальний моральний закон.

Філософія Канта є теоретичною передумовою правової держави, суттю якої є утвердження принципу універсальної відповідальності людини, заснованої на її раціональному та вільному виборі й відповідальності за своє життя.

Макс Вебер також розглядає відповідальність в ракурсі етики, показуючи, що будь-яка людина існує в рамках двох систем координат, підпорядкованих концептуально різним етичним максимумам – "етики переконання" або "етики відповідальності". За логікою етики переконання, людина у своїх вчинках орієнтується на принцип повинності, але в результатах не схильна звинувачувати себе, винним виявляється будь-хто інший: людина, фатум і навіть Бог. Так М. Вебер зазначає, що християнин вчиняє як належить, а щодо результату сподівається на Бога. Цій максимі М. Вебер протиставляє "етику відповідальності", в основі якої лежить усвідомлення людиною необхідності відповідати за будь-які наслідки своїх діянь, не перекладаючи провину за свої невдачі на інших. Етика переконання характерна для релігійної етики, де головним стає прагнення до досконалості, високі цілі і прагнення. Але досягти ідеалу неможливо, тому неможливо нести відповідальність. Етика відповідальності сприймає світ реальний в усіх його проявах, враховує всі недоліки нашого світу. У цьому світі людина сама вибирає цілі і способи їх досягнення, а також несе відповідальність за наслідки свого вибору [8, с. 83].

У XX ст. розвивається нова парадигма відповідальності. Вперше в історії суб'єктами права й відповідальності згідно із законом стали всі люди незалежно від їх гендерних, расових, національних, релігійних і класових відмінностей. Значно розширилось і коло відповідальності, охопивши не тільки економічну, моральну і правову, а й культурну, екологічну відповідальність. Відповідальність набуває темпоральності: з'являється розуміння того, що існує відповідальність за минуле і за майбутнє [9 – 11].

Екзистенціалісти, розглядаючи відповідальність, виходять з того, що бога немає, але є лише буття людини. Так, Ж.П. Сартр виходить з того, що спочатку людина, яка приходить у цей світ, не володіє особистісною сутністю. Вона – всього лише проект самої себе і її "існування передує сутності". Це означає, що людина, перш ніж визначитися, стати самою собою, повинна пройти чималий шлях, сконструювати свою сутність. Саме свободою вибору і можливістю приймати рішення людина відрізняється від усіх інших істот. Кожен має уявлення про те, яким він буде, має потенціал для досягнення цілей. Але людина стає лише тим, ким вона сам себе зробить, тому відповідальність за те, ким вона стала, несе тільки сама.

Ж.П. Сартр вперше вказав на те, що людина несе не тільки відповідальність за саму себе, а й за все людство, оскільки особистісний вибір завжди відображається на суспільстві: "Якщо, з іншого боку, існування передує сутності і якщо ми хочемо існувати, творячи одночасно наш образ, то цей образ є значущим для всієї нашої епохи в

цілому. Таким чином, наша відповідальність є набагато більшою, аніж ми могли б припускати, оскільки поширюється на все людство" [12].

М. Хайдеггер пов'язує відповідальність зі свободою і з турботою. Свобода дана людині від народження, але, отримуючи свободу, людина приймає відповідальність за себе і за світ. Оскільки життя людини залежить від навколишнього світу, то вона повинна піклуватися про нього. Турбота і відповідальність стають умовою існування світу, хоча деякі люди прагнуть сховатися в "анонімному" колективному житті, відмовитися від власної волі, а значить і від відповідальності [13].

Відповідальність завжди була умовою свободи. Людина, звільнена від пут релігії, залишається один на один з реальністю, що вимагає постійного вибору, а також необхідністю відповідати за цей вибір, як перед собою, так і перед суспільством.

У XX столітті проблема відповідальності потрапляє під пильну увагу не тільки філософів, але і вчених з різних галузей науки: соціологів, психологів, педагогів, юристів тощо і це пов'язано, в першу чергу, зі складністю і багатогранністю даного поняття, що, в свою чергу, визначає необхідність комплексного міждисциплінарного дослідження даного феномена, а також пояснює відсутність єдиної позиції про те, що є відповідальність, які її функції, структура.

На даний момент не існує єдиної дефініції цього терміна. Необхідно відзначити, що саме наявність такого великого семантичного поля, що включає такі різноманітні поняття, ознаки та елементи, призводить до того, що в сучасній науці відсутня єдина позиція в розумінні суті відповідальності, а також розглядаються окремо різні ознаки і види відповідальності.

У психолого-педагогічній сфері відповідальність розглядається як базове особистісне утворення, де відповідальність виступає як сприйняття особистістю соціальних норм і вимог і оцінка поведінки особистості з точки зору моралі.

Близьким до розуміння відповідальності є розгляд даного феномена в етиці як моральної категорії.

Правовий підхід розглядає відповідальність з точки зору санкцій за порушення вимог суспільства, втілених у закони.

Найбільш широко даний феномен розглядається у філософії, де зроблені спроби розробити цілісний підхід до розуміння відповідальності, яка не тільки є характеристикою особистості, але і якісною характеристикою всіх суспільних відносин: в економіці, політиці, соціальній сфері, сфері міжособистісної комунікації і т.д.

Також були зроблені спроби визначити види і структуру відповідальності. Зазвичай, основними видами відповідальності вважають: політичну, правову, моральну (моральнісну), індивідуальну (персональну), колективну (суспільну), партійну, громадянську, сімейну і т.д., що дозволяє вести мову про відсутність цілісної класифікації даного феномена.

Є всі підстави стверджувати, що будь-яка відповідальність є соціальною, оскільки є породженням суспільства і можлива лише в суспільстві. Виходячи з цього, як правило, виділяють наступні види відповідальності [8]:

- *за характером відносин* – соціально-економічна, правова, соціально-політична, етична (громадянська, сімейна, матеріальна відповідальність є окремими проявами зазначених видів відповідальності);
- *за характером суб'єкта* – індивідуальна й колективна (суспільна).

Необхідно відзначити, що такий розподіл є умовним. Так, складно уявити собі чисто економічну, правову або політичну відповідальність, оскільки в реальному житті всі види відповідальності тісно взаємопов'язані і взаємозумовлені.

Продовжуючи думку про соціальний характер відповідальності пошлемося на точки зору вітчизняних дослідників даної царини. Так, Н. Крестовська і Л. Матвєєва зазначають, що соціальна відповідальність – це ставлення суспільства до вчинків особи з погляду виконання нею соціальних норм. Вона зумовлюється необхідністю підпорядковувати, координувати та коригувати в процесі спільної діяльності дії кожного з діями інших, приватний інтерес погоджувати із загальним [14].

Соціальні ж норми здійснюють вплив на свідомість і поведінку людей, на відносини між ними через систему оціночного мислення. Тобто норма стає власне критерієм оцінювання: добре – погано; позитивно – негативно. Оцінка вже власне передбачає вибір: добре – потрібно; погано – не потрібно. За допомогою норм соціального характеру здійснюється оцінка вольових дій і наслідків дій людини. Система соціальних норм кожного суспільства містить успадковані від попередніх поколінь оцінки "добра" і "зла", виражені у вигляді норм, інституцій. Соціальні норми – це стабільні узагальнені оцінки звичних для даного суспільства ситуацій, відносин, дій людей. Вони виражають ідеї, ідеали, інтереси, суперечності в суспільстві, в межах якого існують [8, с. 85-86].

На думку С. Бобровник, соціальну відповідальність можна визначити як діалектичний взаємозв'язок між особою та суспільством, що характеризується взаємними правами та обов'язками з виконання приписів соціальних норм та покладенням різноманітних засобів впливу в разі її порушення [15, с. 289-301].

Отже, соціальна відповідальність виникає тоді, коли поведінка індивіда має суспільне значення та регулюється соціальними нормами. У процесі розвитку суспільства складаються відповідні відносини між людьми у вигляді взаємних прав та обов'язків.

Соціальну відповідальність, цілком справедливо, визнають методологічною основою вироблення поняття відповідальності через аналіз співвідношення категорій свободи і необхідності. Відповідальність завжди пов'язана з необхідністю дотримання приписів, правил поведінки, підкорення, узгодження своїх вчинків з об'єктивними законами природи та суспільства. Зокрема, якщо немає необхідності у дотриманні будь-яких норм, приписів, то немає й відповідальності.

Зокрема, А. Плахотний зазначає, що категоріальний аналіз соціальної відповідальності передбачає розкриття діалектичного взаємозв'язку категорій свободи – необхідності – соціальної активності – діяльності – спілкування – способу життя. Потреба з'ясувати міру відповідальності людини за вчинки викликала філософську проблему співвідношення "вільної волі" і зумовленості, окрім волі, проблеми свободи і необхідності в поведінці людини. Проблема свободи виникла при вирішенні питання причинності і, зокрема, такого її особливого випадку, як вільна причина, тобто йшлося не про детермінацію явищ, яка походить від якихось сил природи, а бере початок у розумній, свідомій, цілеспрямованій діяльності людини, в її розумі та волі [16, с. 14].

Варто враховувати, що кожна людина, кожне суспільство буде володіти своїм власним неповторним "малюнком" відповідальності, який буде залежати тільки від того, яка або які види відповідальності превалюють.

Економічну відповідальність можна віднести до базового типу відповідальності, оскільки її можна співвіднести з матеріальними потребами як людини, так і суспільства, що забезпечують фізичне виживання. Індивідуальна економічна відповідальність передбачає обов'язок кожної дієздатної людини бути суб'єктом економічних відносин, брати участь в економічній діяльності (тобто приймати рішення і відповідати перед

суспільством за їх наслідки), що як мінімальна вимога може виражатися в необхідності забезпечувати себе і задовольняти власні потреби.

Колективна економічна відповідальність у першу полягає у вимозі до соціальної групи або організації виробляти товари і послуги, необхідні для забезпечення матеріальних потреб суспільства.

Індивідуальна і колективна правова (юридична) відповідальність, як справедливо зазначає І. Морозова, ієрархічно знаходиться на наступному ступені і означає обов'язок (персональний або колективний) виконувати закони, ставитися до них як документально затверджених правил поведінки в суспільстві [17, с. 27]. Тобто, даний вид відповідальності забезпечує стабільність функціонування соціальної системи в рамках існуючого правового поля.

Політична відповідальність з'являється тоді, коли людина, соціальні групи і суспільство готові не просто дотримуватися встановлених законів держави, а й бути причетними до управління власною державою. Індивідуальна політична відповідальність пов'язана з необхідністю брати участь у політичному житті країни і наявністю громадянської (активної або пасивної) позиції окремої особистості.

Колективна політична відповідальність передбачає необхідність соціальних груп, колективів, у тому числі політичних організацій, державних структур кожному на своєму рівні брати участь у розробці шляху розвитку держави; даний рівень відповідальності вимагає співвіднесення прийнятих рішень з благом суспільства і держави. При цьому індивід розділяє відповідальність за рішення, прийняті особами або структурами, наділеними повноваженнями ці рішення приймати.

Найвищим типом відповідальності є етична, оскільки вимагає не стільки зовнішнього дотримання норм і пристойності, скільки добровільного дотримання моральному закону, в цьому її подібність з обов'язком. Без етичної відповідальності суспільство приречене, оскільки лише вона наповнює істинним сенсом усі інші види відповідальності.

Етична (моральна) індивідуальна відповідальність передбачає наявність двох рівнів – внутрішнього і зовнішнього. Для внутрішнього рівня характерні аналіз індивідом власної поведінки і його співвіднесення з етичними суспільними нормами, правилами і цінностями. У даному випадку особистість відповідає перед внутрішнім "Я", перед власною совістю. Зовнішній рівень передбачає співвіднесення соціальною групою поведінки окремої особистості з встановленими етичними нормами і покарання в разі "аморальної" поведінки з точки зору конкретного суспільства. Колективна етична відповідальність можлива як за колективні проступки, так і відповідальність колективу або соціальної групи за невідповідну поведінку окремої людини.

Ханна Арендт, розглядаючи проблему колективної відповідальності, зазначає: "Є дві необхідні умови колективної відповідальності: я повинен вважатися відповідальним за щось, чого не робив, і я повинен нести таку відповідальність в силу свого членства в групі (колективі), яке неможливо припинити добровільним актом з мого боку, тобто членства, вкрай несхожого на ділове партнерство, яке я завжди вільний припинити" [5, с. 207]. Відповідальність цього роду завжди носить політичний характер і спільнота вважається відповідальною за те, що було зроблено від її імені. Опосередкована відповідальність за дії, яких ми не робили, за наслідки того, в чому немає нашої провини, є нашою платою за той факт, що ми живемо не самі по собі, а серед інших людей. І важливо те, що ця відповідальність має не тільки безособовий, але і особистісний характер [4, с. 61].

Оскільки відповідальність пов’язана не тільки з необхідністю виконувати певні суспільні очікування, функції та прийняттям рішень, але й з обов’язком відповідати перед суспільством за ці рішення, то за характером санкцій можна виділити два основних типи відповідальності: етичну (моральну), юридичну (цивільну, адміністративну, кримінальну). Тобто, за невиконання взятих чи покладених на людину або соціальну групу обов’язків (що відповідає різним типам відповідальності за відносинами: економічній, правовій, політичній) можуть настати два типи вищезазначених санкцій. Так, безвідповідальна поведінка людини або колективу може спричинити різне за ступенем “тяжкості” покарання – від громадського осуду до страти – незалежно від того, якої сфери відповідальності воно стосується. Як приклад наведемо виключення за часів родоплемінних відносин з роду деяких порушників батьківської волі (що відповідає етичній відповідальності) з подальшим їх вигнанням з території проживання роду, що найчастіше (з урахуванням етапу розвитку суспільства) було рівнозначно страті. В даний час небажання виконувати вимоги батьків може спричинити громадський осуд або взагалі розцінюватися як прояв свободи особистості.

Виділення колективної відповідальності вимагає висвітлити два основні підходи до розуміння даного виду відповідальності. Умовно перший підхід можна позначити як індивідуалістичний (основним представником якого є Карл Поппер) і колективістський (Карл Маркс). Так, К. Поппер розглядає колективну відповідальність як сукупність індивідуальних відповідальностей, де індивідуальна відповідальність є ключовою. Якщо розглядати колективну відповідальність як суперпозицію множин (індивідуальностей), то залежно від конфігурації цих суперпозицій формуватиметься нова множина, яка зазнаватиме змін щоразу, як буде змінюватися кількість членів суспільства і те, як і яку саме відповідальність вони несуть. Дана концепція протиставляється концепції колективності в марксистській традиції, де групова відповідальність розподіляється між усіма членами суспільства. Кардинальна відмінність даних концепцій полягає у тому, що відповідальність “делегованих” суспільством завжди відповідає завданням суспільства в цілому, і передбачає наявність відповідальності, обумовленої і схваленої суспільством. У разі неможливості будь-яких членів суспільства (або цілої групи) виконувати покладені на них завдання (тобто нести відповідальність), відбудеться автоматичний перерозподіл обов’язків, що неможливо при індивідуалістському підході.

Цілком очевидно, що в сучасному світі ці дві концепції повинні поєднуватися, тобто, в сучасному суспільстві повинні співіснувати колективна відповідальність як певна сукупність суспільних вимог і очікувань, яка б визначала вектор суспільного розвитку й індивідуального руху, а також максимізація індивідуальної відповідальності, яка б виявлялася в крайньому ступені готовності особистості відповідати за наслідки своїх рішень і дій, і яка б не дозволила колективній відповідальності перетворитися в “кругову поруку”.

Разом з тим, всебічна криза відповідальності у поєднанні з глобалізацією призводить до того, що рішення, прийняті на рівні окремих держав, є вкрай безвідповідальними не тільки по відношенню до власного суспільства, а й по відношенню до інших держав.

Висновки.

Таким чином, основною тенденцією в інформаційному суспільстві стає повсюдний відхід від відповідальності фактично на всіх рівнях її прояву, що дозволяє вести мову про асиметричність розвитку суспільства: при надзвичайно високому ступені технологічного розвитку відбувається деградація етики і моралі. Це стає основною суперечністю, що продукує соціальні конфлікти різного штибу: від міжособистісних до

міждержавних. Глобалізація, як процес, що супроводжує інформаційно-технологічну революцію, призводить до глобалізації безвідповідальної поведінки, а також до глобалізації наслідків такої безвідповідальності. При існуючих протиріччях і конфліктах є очевидним, що глобальна безвідповідальність стає не тільки загрозою окремим особистостям або соціальним групам, але й усім соціальним системам, а також планеті в цілому. Цілком очевидно, що ступінь відповідальності повинен бути прямо пропорційним можливостям (у першу чергу технічним) суспільства, що суспільству необхідно переглянути систему моральних цінностей, виробити механізми захисту, в основі яких повинен знаходитись принцип відповідальності. Цей принцип повинен мати на увазі максимізацію всіх видів і рівнів відповідальності, а також, з урахуванням взаємозалежності всіх елементів соціуму і залежності природи від дій людини, вироблення міждержавної етичної концепції, яка б визначила трансформацію економічних, політичних і правових відносин.

Як цілком справедливо стверджував свого часу Г. Берман: "Як моральна необхідність знайти рівновагу між індивідуалізмом і комунітаризмом, так і політична необхідність знайти таку рівновагу в інтересах домінуючих інститутів у конкретному державному устрої повинні оцінюватися у світлі довготривалого історичного розвитку, коли такі моральні й політичні питання виникають. Привнесення довгострокової тимчасової перспективи у філософську та політичну аргументацію істотно змінює її характер" [18, с. 301].

Використана література

1. Прудникова О.В. Феномен інформаційної культури: онтологічний статус та соціоантропологічні детермінанти: монографія / за заг. ред. О.П. Дзьобаня. Харків: Право, 2017. 496 с.

2. Дзьобань О.П., Мануйлов Є.М. Бінарна опозиція "свобода-відповідальність" в інформаційному суспільстві: до постановки проблеми. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія*. 2016. № 1 (28). С. 15-26.

3. Аристотель. Соч. в 4 т. / пер. с древнегреч. Т. 4. Москва: Мысль, 1983. 830 с.

4. Осипов И.Д. Парадигма ответственности в европейской философии. *Вестник СПбГУ*. Сер. 17. 2014. Вып. 2. С. 52-63.

5. Арендт Х. Ответственность и суждение. Москва: Изд-во Института Гайдара, 2013. 352 с.

6. Дзьобань О.П., Жданенко С.Б. Ідея теократичного панування у вченні Августина Блаженного та її практичне втілення у середні віки. *Наукові записки Харківського університету Повітряних Сил. Соціальна філософія, психологія*. 2007. Вип. 3 (29). С. 30-38.

7. Гоббс Т. Левіафан. Москва: Мысль, 2001. 478 с.

8. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології: монографія / І.В. Арістова, О.А. Баранов, О.П. Дзьобань та ін.; за заг. ред. проф. К.І. Бєлякова. Київ: КВІЦ, 2019. 344 с.

9. Буященко В. Соціальна відповідальність: від дискурсу до практики. *Вісник Академії праці, соціальних відносин і туризму*. 2017. № 1. С. 6-10.

10. Діденко Л.В., Кондрашова-Діденко В.І. Соціостудії: відповідальність. *Актуальні проблеми філософії та соціології*. 2017. Вип. 17. С. 22-24.

11. Фоменко А.М. Свобода та відповідальність особистості: дискурс сучасності. *Стратегія розвитку України*. 2017. № 1. С. 7-10.

12. Сартр Ж.П. Экзистенцианализм – это гуманизм. URL: https://scepsis.net/library/id_545.html (дата звернення 17.10.2019).

13. Хайдеггер М. Бытие и время. URL: http://yanko.lib.ru/books/philosoph/haydegger-butie_i_vremya-8l.pdf (дата звернення 10.10.2019).

14. Крестовська Н.М., Матвеева Л.Г. Теорія держави і права: Елементарний курс. 2-е вид. Харків: ТОВ "Одіссей", 2008. 432 с.

15. Загальна теорія держави і права: (основні поняття, категорії, прав. конструкції та наук. концепції): навч. посіб. / за ред. О.В. Зайчука, Н.М. Оніщенко. Київ: Юрінком Інтер, 2008. 400 с.

16. Плахотный А.Ф. Проблеми социальной ответственности. Харків: Вища школа, 1981. 190 с.

17. Морозова И.С. Кризис ответственности в контексте развития культуры информационного общества / И.С. Морозова: дис. …канд. филос. наук. Москва, 2014. 191 с.

18. Берман Г.Д. Вера и закон: примирение права и религии. Москва: Ad Marginem, 1993. 431 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.727/.729 (477+430+061.1ЄС)

КОСІЛОВА О.І., *кандидат політичних наук, доцент,* юридичний факультет Київського національного університету ім. Тараса Шевченка
ФЕДІРКО І.П., *кандидат філософських наук, доцент*, доцент кафедри політології Київського національного університету ім. Тараса Шевченка

ПРАВА І СВОБОДИ ЛЮДИНИ І ГРОМАДЯНИНА: КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО ДИФЕРЕНЦІАЦІЇ В ФРН ТА УКРАЇНІ

Анотація. *В статті аналізується співвідношення прав людини і громадянина загалом та в Україні та ФРН зокрема. Досліджуються основні підходи до класифікації прав людини. Наголошується, що на відміну від прав людини, які поширюються на всіх осіб без обмежень, права громадянина охоплюють сферу правовідносин індивіда з державою, яка характеризується наявністю громадянства. Наголошується на тому, що у ФРН свободи є частиною прав особи і визначаються як "права на свободи", маючи при цьому негативний статус, що передбачає мінімізацію державного впливу та втручання. Аналізується правовий статус іноземців в обох країнах та особливості реалізації ними своїх прав та свобод.*

Ключові слова: *права людини, права громадянина, права іноземців, права кожного, права громадян Німеччини, права громадян України, права громадян ЄС.*

Summary. *The article analyzes the relationship between human rights and rights of citizens in general and in Ukraine and Germany particular. Basic approaches to the classification of human rights are explored. It is emphasized that, unlike human rights, which apply to all persons without restriction, the rights of the citizen cover the sphere of legal relations of the individual with the state, characterized by the presence of citizenship. It is emphasized that in Germany the freedoms are part of the rights of individuals and are defined as "rights to liberties", while having a negative status, which implies minimization of state influence and interference. The legal status of foreigners in both countries and the peculiarities of the exercise of their rights and freedoms are analyzed.*

Keywords: *human rights, rights of citizens, rights of foreigners, rights of everyone, rights of citizens of Germany, rights of citizens of Ukraine, rights of EU citizens.*

Аннотация. *В статье анализируется соотношение прав человека и гражданина в целом и в Украине и ФРГ в частности. Исследуются основные подходы к классификации прав человека. Отмечается, что в отличие от прав человека, которые распространяются на всех лиц без ограничений, права гражданина охватывают сферу правоотношений индивида с государством, которая характеризуется наличием гражданства. Подчеркивается, что в ФРГ свободы являются частью прав личности и определяются как "права на свободы", имея при этом отрицательный статус, предусматривающий минимизацию государственного влияния и вмешательства. Анализируется правовой статус иностранцев в обеих странах и особенности реализации ими своих прав и свобод.*

Ключевые слова: *права человека, права гражданина, права иностранцев, права каждого, права граждан Германии, права граждан Украины, права граждан ЕС.*

Постановка проблеми. У зв'язку з процесами глобалізації у світі та посиленням тенденцій до універсалізації прав, створенням нових міждержавних утворень та союзів, поступово стираються межі між різними конституційно-правовими статусами особи, розширюється перелік загальнолюдських прав, виникають нові види прав та свобод. Одним з найбільш поширених підходів до класифікації прав і свобод у сучасній юридичній науці є їх розмежування на права і свободи людини і громадянина. Інколи ці терміни вживаються як альтернативні, інколи як близькі за змістом. Тим не менш, між

ними існують суттєві відмінності як у змісті, так і в обсязі. У зв'язку з цим, здійснення порівняльного аналізу прав і свобод людини та громадянина у Федеративній Республіці Німеччина, яка є членом Європейського Союзу (далі – ЄС), та в Україні, яка визначила вступ до нього як головний вектор зовнішньополітичного розвитку, є доречним та актуальним завданням.

Серед сучасних вітчизняних науковців дослідження прав та свобод людини та громадянина здійснювали низка вчених, серед яких П.М. Рабінович, Р.С. Мельник, В.П. Колісник, Ю.Г. Барабаш, Ю.І. Римаренко, У.В. Ільницька, А.С. Пазенок, Н.Г. Шукліна, А.М. Колодій, О.В. Совгиря, С.П. Головатий, В.Л. Федоренко, А.Ю. Олійник, М.В. Савчин, М.М. Антонович, В.П. Шаповал та інші. Серед сучасних німецьких дослідників у цій сфері варто відзначити Ганса Д. Яраса, Гадули Гезер, Бернгарда Вілса, Жозефа Шустера, Петера М. Хюбер, Мартіна Кюніха та інших.

Метою статті є компаративне дослідження змісту та обсягу прав людини і громадянина в ФРН та Україні, визначення сучасних тенденцій їх розвитку.

Виклад основного матеріалу. Права і свободи особи є одним з центральних елементів її конституційно-правового статусу. Поділ прав і свобод за суб'єктами на права і свободи людини і громадянина у конституційній теорії і практиці нерідко ототожнюються з поділом на особисті та політичні права. Як зазначає В.П. Шаповал, дуалізм особистих та політичних прав і свобод як прав людини і громадянина має важливе загальнополітичне і конституційне значення. На основі аналізу розмежування цих прав і свобод та з урахуванням практики їх реалізації можна зробити висновки щодо характеру співвідношення суспільства і держави у конкретній країні, природи існуючого тут політичного режиму [1, с. 113].

Український науковець, конституціаліст М.В. Савчин вважає, що закріплення найважливіших положень щодо визнання пріоритету прав і свобод людини щодо державних та інших інтересів, а також визнання людини, її життя і здоров'я, честі і гідності, недоторканності і безпеки найвищою соціальною цінністю, розміщення у спеціально присвяченому правам людини II Розділі Конституції України майже третини статей від загальної їх кількості, свідчить про достатньо високий рівень визнання і формування конституційного статусу людини та громадянина в Україні [2, с.124].

Предметом аналізу даної статті є дослідження відмінностей у змісті та обсязі прав і свобод людини і громадянина в ФРН та в Україні. Для реалізації поставленої мети необхідно з'ясувати зміст категорії "людина" та "громадянин". У найбільш широкому розумінні людина – жива, наділена інтелектом істота, суб'єкт суспільно-історичної діяльності і культури [3]. Синонімами поняття "людини" є особа, особистість, індивід, поняття що підкреслюють певні соціально-культурні особливості та природні здібності особи. Тоді як громадянин – це житель певної території держави або країни. Громадяни в кожній країні становлять найчисленнішу категорію населення та наділені правами і свободами в найбільш широкому обсязі. Ця приналежність є юридично закріпленою.

Таким чином, ми погоджуємося з думкою українських науковців В.М. Бесчастного, О.В. Філонова, В.М. Субботіна, С.М. Пашкова, що права людини випливають з самої природи людини, тоді як права громадян визначаються фактом громадянства [4, с. 72].

В українській правничій науці категорія "права" найчастіше визначається як "певні можливості людини, необхідні для її існування та розвитку у конкретно-історичних умовах, які об'єктивно зумовлюються досягнутим рівнем розвитку людства і мають бути загальними та рівними для всіх людей" [5, с. 16].

У більш широкому розумінні термін "право" у тому значенні, яке він має в словосполученні "права людини", виходить за межі тільки певних можливостей людини,

необхідних для її існування та розвитку в конкретно-історичних умовах, як він тлумачиться у вітчизняній юридичній науці. Цей термін може означати також: вимогу, претензію, привілей тощо [6, с. 20].

Слід згадати, що саме поняття "права людини" з'явилося в епоху буржуазних революцій. Зокрема, перше тлумачення понять права людини та права громадянина було здійснено у Декларації прав людини і громадянина від 14 липня 1789 року у Франції. У цьому історичному документі, який ліг в основу наступних міжнародно-правових документів та конституцій, було закріплено основоположні цінності, що визначали конституційно-правовий статус особи. Зокрема, у ст. 1 Декларації було проголошено: "Людина народжується вільною і рівною в правах, і залишається такою". У ст. 2 визначено головну мету держави: "Мета всіх політичних суспільств – збереження природних і невідчужуваних прав людини, прав, які є свободою, власністю, безпекою та правом протистояти свавільному гнобленню". У ст. 4 зазначено: "Свобода полягає у тому, що можна робити все, що не завдає шкоди іншій людині. Таким чином, здійснення природних прав кожної людини має лише ті межі, які гарантують іншим членам суспільства однакові права. Ці межі можуть визначатися виключно законом" [7].

Положення зафіксовані у Декларації прав людини і громадянина заклали основу нового політичного мислення та мали вплив на всю Європу. Відтоді у багатьох конституціях європейських держав було зафіксовано принцип вроджених, невідчужуваних та основоположних прав людини, які мають захищатися від втручання з боку держави. Отже, права людини, або права кожного – це такі основоположні права, які не передбачають обмежень щодо кола осіб (адресатів).

Права особи безпосередньо пов'язані зі свободами. Традиційне для зарубіжного конституціоналізму тлумачення свободи полягає в тому, що її звичайно сприймають як відсутність широких обмежень діяльності особи. Але це не означає абсолютної свободи. Держава встановлює певні вимоги, яким повинна відповідати діяльність кожної особи. Межею свободи будь-якої людини є свобода інших людей. Іноді свобода розглядається не як загальний принцип, а як одне з конкретних прав особи – право на свободу. Зокрема, такі формулювання можна знайти в конституціях Іспанії та Японії. Це має історичну традицію: декларації прав і свобод, проголошені у XVIII ст., фактично відносили до особистих прав і свобод право на життя, свободу, рівність і забезпечення людської гідності [1, с. 113].

У Конституції ФРН, подібно до Іспанії та Японії, категорія свободи розглядається крізь призму прав, тобто як права на свободи. Основним призначенням основоположних прав на свободи є "забезпечення захисту сфери особистої свободи від втручання з боку публічної влади" [8]. Таким чином, права на свободи гарантують "свободу від держави". Оскільки права на свободу традиційно в першу чергу спрямовані на захист від втручання держави, в них переважає захисна функція. Саме тому їх ще називають "оборонними правами" [8].

Свобода як принцип деталізується у проголошених в конституціях особистих правах і свободах. Останні тісно пов'язані з поняттям процесуальних гарантій прав і свобод. Деякі автори виділяють процесуальні гарантії в окрему групу особистих прав – прав обвинуваченого в судовому процесі. Проте зміст процесуальних гарантій ширший. Він охоплює не тільки процедури судочинства, а й попередні процесуальні стадії [1, с. 114].

У сучасній вітчизняній юридичній науці застосовуються різні критерії для класифікації основоположних прав та свобод. За характером потреб людини, які забезпечуються правами, П.М. Рабінович пропонує поділяти права людини на фізичні (життєві), особистісні, культурні (гуманітарні), економічні та політичні [5, с. 19].

Українська дослідниця М.М. Антонович зазначає, що родове поняття “права людини” поділяється на видові поняття за різними критеріями, і різні терміни використовуються для специфікації цього поняття. Зустрічаємо терміни “права людини” і “права громадянина”. Природно, викликає подив, коли ці поняття використовуються в сполученні “права людини і громадянина”, так, ніби громадянин не є людиною. З іншого боку, очевидно, що поняття “права людини” та “права громадянина” не є синонімами, оскільки не кожна людина має громадянство за внутрішньодержавним правом, а, отже, не користується деякими правами, які надаються тільки громадянам певної держави [9, с. 23].

Загалом, найбільш поширеними критеріями класифікації прав і свобод людини і громадянина в українській юридичній науці є їх диференціація за:

- суб’єктами (на права людини та громадянина);
- за видом суб’єкта (на індивідуальні та колективні);
- за ґенезою (на природні і похідні);
- за черговістю їх включення у Конституцію (на права першого, другого та третього поколінь);
- за ступенем їх абсолютизації (на такі, що підлягають обмеженням, і такі що їм не підлягають);
- за характером утворення (на основні (конституційні) та доповнюючи (конкретизуючі);
- за змістом (на громадянські/особисті, політичні, економічні, соціальні, культурні [10, с. 110; 11, с. 132].

Отже, у найбільш загальному розумінні права людини слід розуміти як права, що належать кожній людині незалежно від її положення (статусу) в державі, суспільстві, сім’ї, професії, від релігійних, світоглядних поглядів та культурних цінностей. Тобто, права людини належать кожній людині в силу того факту, що вона народжена людиною. Інші характеристики, такі як колір шкіри, стать, мова, політичні чи інші ідеологічні переконання, національне чи соціальне походження не можуть вплинути на чинність прав людини, пов’язаних із людським існуванням. Права людини є природними та невідчужуваними.

Аналіз вітчизняної юридичній літературі засвідчує, що під правами людини найчастіше розуміють особисті права людини, які визначають як громадянські [10, с. 95-97]. До них як правило відносять: право на життя (ст. 27), на вільний розвиток особистості (ст. 23), повагу гідності (ст. 28); право на особисту недоторканність (ст.29); право на недоторканність житла (ст. 30), право на свободу думки і слова (ст.34), світогляду та віросповідання (ст. 35); право на свободу пересування (ст. 33), вільний вибір місця проживання (ст. 33); право на справедливий неупереджений суд та правову допомогу (ст. 55); право захищати своє життя і здоров’я від протиправних посягань (ст. 55), право на підприємницьку діяльність (ст. 42), право на працю (ст.43) тощо [12].

Таким чином, можемо констатувати, що в українській юридичній літературі громадянські права визначаються як особисті (або людські), тобто такі, що поширюються на всіх людей, незалежно від національності, мови, статі, походження, конституційно-правового статусу тощо.

У зв’язку з окупацією частини території України на Сході, а також території Автономної Республіки Крим військами Російської Федерації, громадяни України, які перебувають на непідконтрольній Україні території зазнають значних утисків та обмежень. В першу чергу це стосується права на життя, тілесну недоторканність, свободи пересування, права власності, прав на соціальний захист, а також політичних прав, зокрема виборчих. Запроваджений українською державою механізм переселення громадян України

на її материкову частину та надання особам статусу тимчасово-переміщених осіб не забезпечує повноцінну реалізацію їх прав та свобод.

Відповідно до німецької правової доктрини, причиною існування прав всіх людини є людська гідність. В ст. 1 Основного Закону ФРН зазначено: "Гідність людини непорушна. Поважати і захищати їх є обов'язок всіх державних органів". Цим твердженням починається преамбула не тільки розділу основоположних прав, але ним пронизано і весь текст Основного Закону [13]. Право гідності є "основою кожної людської спільноти, миру і справедливості в світі" [14, с. 92]. Фундаментальні права є основоположними правами свободи та рівності, що надаються особам по відношенню до держави та мають конституційний статус. Основоположні права є невід'ємними, постійними і закріпленими. Кожен може посилатися на захист своїх прав проти держави. Ці права закріплено у тексті Основного Закону як права "кожного", "будь-кого", "нікого" або "всіх людей". За допомогою здійснення правосуддя надаються юридичні гарантії основоположних прав, забезпечується право бути заслуханим у суді та встановлюються фундаментальні заборони, такі як заборона зворотної дії закону, а також подвійне покарання. Основоположні права регулюються Федеральною конституцією а також конституціями земель [15].

У Конституції ФРН права людини можна визначити за такими термінами, як "кожен", "всі люди", "ніхто" [14, с. 22]. Центральною категорією у доктрині прав людини у ФРН є гідність як безумовне визнання кожної особистості носієм рівної свободи, використання якої повинно бути дозволено незалежно від волі інших людей. У такому розумінні, права людини не створені державними нормами, а мають бути визнані ними лише як щось існуюче.

Перелік загальнолюдських прав у Німеччині є подібним до вітчизняних: право на свободу дій, на життя, на фізичну недоторканність, на вільний розвиток особи (ст. 2, ст. 104), право на рівність (ст. 3), свобода висловлення та поширення своєї думки; свобода преси та теле-, радіомовлення (ст. 5); право на шлюб та створення сімії, батьківські права, охорона материнства (ст.6, ст.7(2); свобода об'єднання (ст. 9(3), право на збереження таємниці листування та телекомунікації (ст. 10); захист від примусової праці (ст. 12(2) та (3)); недоторканність житла (ст. 13), майнове та спадкове право (ст. 14); право петицій (ст. 17), гарантії судового захисту (ст. 4), основоположні права в суді (ст. 103), право на притулок (для іноземців) (ст. 16а) [13]. У німецьких джерелах громадянські права визначаються як права, які належить громадянину або члену громади і стосуються відносин між державою та громадянином (народом) [15].

У Федеративній Республіці Німеччина громадянські права містяться в Основному Законі. Разом з правами людини вони утворюють систему основоположних прав. Однак, слід зазначити, що не всі права слід розглядати як громадянські права, а лише ті, які належать німцям. Згідно з ст. 20 Основного Закону джерелом державної влади є народ, а до (німецького) народу відносяться всі ті, хто має німецьке громадянство (ст. 116) [13]. Тому у ФРН громадянські права в Німеччині також називають "правами німців".

Відповідно до Основного Закону ФРН громадянські права стосуються німців. Громадянські права (тобто права громадян), включають у себе право на участь у житті держави шляхом надання активного та пасивного виборчого права, права обіймати державні посади; право вільного пересування по всій федеральній території, захист від позбавлення громадянства, право на повстання. Крім того, громадянські права включають права на участь у житті місцевої громади, спільно користуватися державними установами та разом із тим, мати певні обов'язки у громаді [15]. Це видно з формулювання: "Усі німці мають право вибирати професію, робоче місце і навчальний центр" (ст. 12(1).

На іноземців не поширюються права німців. Щодо них діє загальний захист, передбачений ст. 2(1) Основного Закону: "Кожен має право на вільний розвиток своєї особистості, наскільки він не порушує прав інших людей і не порушує конституційний порядок чи моральний закон" [13]. Іноземці у Німеччині можуть звертатися до суду щодо недотримання принципів правової держави (зокрема, пропорційності, дискреційних безпомилкових рішень, захист довіри). На ці підстави поширюється дія основоположних прав, закріплених у ст. 19(4), 101(1), 103(1) Основного Закону [14, с. 25].

На думку німецької дослідниці Гадули Гезер, поділ прав у Німеччині на права людини та права громадянина є значною мірою умовним, тому що іноземцям доступними є більшість прав громадян Німеччини, за виключенням деяких. Виключно громадянам Німеччини належать такі права, як свобода зборів (ст. 8), свобода пересування в межах Німеччини (ст. 11), свобода вибору професії, робочого місця, навчального закладу (ст. 12(1)), безперервність громадянства, заборона екстрадиції (ст. 16), право на опір (ст. 20), права рівності у громадянських правах та обов'язках, право доступу до державної служби та державних посад (ст. 33(1) – (3) [16].

Особливістю правового регулювання прав і свобод у Конституції ФРН, що відрізняє її від Конституції України, є закріплення права німців (громадян Німеччини) на повстання, згідно зі ст. 20, п. 4 "Проти всіх, хто виступає проти існуючого конституційного ладу, усі німці мають право чинити опір, якщо інший засіб неможливий" [13]. Тоді як у ст. 44. абз.1, 2 Конституції України лише зазначено, що: "Ті, хто працює, мають право на страйк для захисту своїх економічних і соціальних інтересів. Порядок здійснення права на страйк встановлюється законом з урахуванням необхідності забезпечення національної безпеки, охорони здоров'я, прав і свобод інших людей" [12].

Досить проблемним у ФРН залишається питання щодо того, якою мірою громадяни ЄС можуть користуватися правами німців. Відповідно до ст. 18(1) "Договору про функціонування ЄС", громадянин ЄС не може бути дискримінований за ознакою свого громадянства. Тому суперечливим є те, наскільки громадянин ЄС може посилатися на і права громадян Німеччини. З одного боку, права німців мають стосуватися і громадян ЄС. Обґрунтування ґрунтується не тільки на забороні дискримінації, а й на загальному застосуванні пріоритету європейського права та так званому принципі "effet-utility", згідно з яким права німців повинні тлумачитися відповідно до європейського законодавства. З іншого боку, застосування прав німців до громадян ЄС нівелює конституційне обмеження щодо захисту прав німців. У будь-якому випадку громадяни ЄС повинні відчувати аналогічний ступінь захисту основоположних прав відповідно до ст. 2(1) Основного Закону [15].

У ЄС також визначені інші громадянські права у "Хартії основоположних прав Європейського Союзу" в ст. 39 – 46, такі як виборче право в ЄС та місцеві вибори, право на добре врядування (gute Verwaltung), закон про доступ до документації, право петицій, право на вільний рух та дипломатичний захист та право звернення до Омбудсмана.

Порівнюючи права громадян України із правами іноземців, слід зазначити, що відповідно до ст. 26 Конституції України, "іноземці та особи без громадянства, що перебувають в Україні на законних підставах, користуються тими самими правами і свободами, а також несуть такі самі обов'язки, як і громадяни України, за винятками, встановленими Конституцією, законами чи міжнародними договорами України" [12]. Таким чином, у Конституції України фактично втілена ідея, що права і свободи кожної людини повинні поважатися кожною державою незалежно наявності чи відсутності в особи статусу громадянина цієї держави [17].

Таким чином, формулювання прав і свобод іноземців в Україні фактично є ідентичним з визначеними правами іноземців в Німеччині. Хоча деякі відмінності все ж таки виявляються при їх більш глибокому аналізі. Зокрема, аналіз відповідних положень Конституції України та Закону України "Про правовий статус іноземців" показує, що іноземці не обмежуються в праві: займатися інвестиційною та підприємницькою діяльністю; на приватну власність; на відпочинок; на соціальний захист (як правило, відповідно до міжнародних договорів України); на користування досягненнями культури; на свободу совісті; на свободу і особисту недоторканність, недоторканність житла, захист від втручання в особисте і сімейне життя, таємницю листування, телефонних розмов і телеграфних повідомлень; на повагу до гідності; на звернення до суду та, якщо інше не передбачено міжнародними договорами, до інших державних органів для захисту їх майнових та немайнових прав [18].

Законами України встановлені також особливості здійснення іноземцями та особами без громадянства права на свободу пересування, вільний вибір місця проживання, права вільно залишати територію України. Відповідно до Закону "Про правовий статус іноземців", іноземці можуть пересуватися по території України і обирати місце проживання в ній тільки в порядку, встановленому Кабінетом Міністрів України.

Іноземці в Україні позбавлені більшості політичних прав. Зокрема, вони не мають права бути засновниками і членами політичних партій, проте, можуть бути засновниками і членами громадських організацій. Іноземці в Україні не можуть обирати і бути обраними до органів державної влади та самоврядування, а також брати участь у референдумах; бути державними службовцями, у тому числі військовослужбовцями. На відміну від громадянина України, іноземця (особу без громадянства), відповідно до закону, може бути видворено за межі України [19]. Іноземці в Україні мають право на звернення, право брати участь у зборах, мітингах, демонстраціях, якщо вони не переслідують політичну мету.

Висновки.

Підсумовуючи вищесказане, зазначимо, що поняття "права людини" вживається у широкому і вузькому значенні. В широкому розуміння права людини охоплюють весь спектр, найширший комплекс прав і свобод особи та їх види. У вузькому значенні, під правами людини розуміються тільки ті права, що не надаються, а лише охороняються і гарантуються державою, діють незалежно від їх конституційно-правового закріплення і державних кордонів.

Важливість прав і свобод не можна применшувати, адже громадянські права обмежують втручання держави у життя людини і підкреслюють найвищу соціальну цінність людини в державі, забезпечують автономію особи від держави, визначають юридичну захищеність людини від будь-якого незаконного втручання у приватне життя, від придушення державою прав і свобод громадянина; передбачають заходи судового захисту кожній людині у випадку порушення її прав.

Права громадян України становлять окрему категорію прав, які закріплені за особами, які володіють громадянством України. Громадянам України належить повний перелік прав і свобод, визначений в Основному Законі. Певні обмеження можуть стосуватися виключно дієздатності особи.

Відповідно до німецької доктрини права, фундаментальні права є основоположними правами свободи та рівності, що надаються особам по відношенню до держави та мають конституційний статус, а основоположним правом для всієї іншої групи прав є право на гідність. В українській правовій доктрині як основоположні цінності визначено право на життя, честь, гідність людини, її безпека та недоторканність.

Загалом, поділ прав на “права людини” та “права громадянина” у Німеччині та в Україні є значною мірою умовним, тому що іноземцям доступними є більшість прав громадян, крім більшості політичних прав. Виключення становлять виборчі права для громадян ЄС у Німеччині, які мають право голосувати на місцевих виборах та на європейських виборах.

Використана література

1. Шаповал В.М. Конституційне право зарубіжних країн: підручник. Київ: Артек, 2002. 264 с.

2. Савчин М.В. Конституційне право України: підручник / відп. ред. проф., д.ю.н. М.О. Баймуратов. Київ: Правова єдність, 2009. 1008 с.

3. Людина. URL: https://uk.wikipedia.org/wiki/%D0%9B%D1%8E%D0%B4%D0%B8%D0%BD%D0%B0#cite_note-%D0%91%D0%AD%D0%A1-2 (дата звернення 31.10.2019)

4. Конституційне право зарубіжних країн: навч. посібник / за ред. В.М. Бесчасного. Київ: Знання, 2008. 467 с.

5. Рабінович П. Основні права людини: поняття, класифікації, тенденції. *Укр. часопис прав людини*. 1995. № 1. С.14-22.

6. Антонович М. Юридична термінологія з прав людини: походження, тлумачення, функціонування. *Укр. часопис прав людини*. 1997. № 3 – 4. С. 19-26.

7. Geschichte der Menschenrechte. URL: https://www.planet-wissen.de/geschichte/menschenrechte/geschichte_der_menschenrechte/pwwbgeschichtedermenschenrechte100.html (дата звернення: 27.09.2019).

8. Funktionen der Grundreche – Arten und funktionen in der Ubersicht. URL: https://www.juracademy.de/grundrechte/grundrechte-arten-funktionen-uebersicht.html (дата звернення 26.10.2019).

9. Антонович М. Україна в міжнародній системі захисту прав людини. Київ: Видавничий дім “КМ ACADEMIA” 2000. 139 с.

10. Конституційне право України: підруч. для студ. вищ. навч. закл. / за заг. ред. В.П. Колісника та Ю.Г.Барабаша. Харків: Право, 2008. 416 с. С. 110.

11. Совгиря О.В., Шукліна Н.Г. Конституційне право України. Повний курс: навч. посіб. Київ: Юрінком Інтер, 2018. 556 с. С.132.

12. Конституція України. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

13. Grundgesetz für die Bundesrepublik Deutschland. URL: https://www.gesetze-im-internet.de/gg/GG.pdf (дата звернення 18.06.2019).

14. Schmidt R. Grundrechte sowie die grundzuge der Verfassungsbeschwerde/Grasberg bei Bremen 2015, 430 s.

15. Bürgerrechte im GG. URL: https://www.juraforum.de/lexikon/buergerrecht (дата звернення 24.09.2019).

16. Gudula Geuther Besondere Merkmale der Grundrechte Informationen zur politischen Bildung Nr. 305/2013, S.13. URL:http://www.bpb.de/157699/grundrechte-in-der-europaeischen-union (дата звернення 04.06.2019).

17. Великий енциклопедичний юридичний словник / за ред. Ю.С. Шемшученка. Київ: ТОВ “Видавництво “Юридична думка”. 2007. С. 385.

18. Про правовий статус іноземців та осіб без громадянства: Закон України. *Відомості Верховної Ради України*. 2012. № 19 – 20. Ст. 179. URL: https://zakon.rada.gov.ua/laws/show/3773-17 (дата звернення 18.06.2019)

19. Права іноземців та осіб без громадянства. URL: https://pidruchniki.com/16011013/pravo/prava_inozemtsiv_osib_bez_gromadyanstva (дата звернення 18.06.2019).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 340:1+347.9

СОЛОНЧУК І.В., старший викладач кафедри інформаційного права та права інтелектуальної власності Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

ІНФОРМАЦІЙНІ ПРАВОВІДНОСИНИ: ПОНЯТТЯ ТА ОХОРОНА

Анотація. *Стаття присвячена інформаційним правовідносинам як унікальному соціальному явищу, їх нормативному регулюванню та охороні. Незважаючи на підвищений науковий інтерес, інформаційні правовідносини як юридична категорія, потребують подальшого дослідження, адже сьогодні є багато дискусійних питань, які ще не врегульовані законодавцем. Представлено систематизація чинників, які визначають недостатній рівень дослідження інформаційних правовідносин на сучасному етапі, виконаний аналіз наукових визначень поняття "інформаційні правовідносини", запропоноване авторське визначення поняття "інформаційні правовідносини", названі їх ознаки та особливості.*

Ключові слова: *інформація, право на інформацію, інформаційні правовідносини, судочинство, правосуддя, охорона інформаційних правовідносин.*

Summary. *The article is devoted to information legal relations as unique social relations, their statutory regulation and protection. Despite the increased scientific interest, information relations as a legal category need further investigation, as there are many debates that have not yet been regulated by the legislator.. The article systematizes the factors that determine the insufficient level of study of information legal relations at the present stage, the analysis of scientific definitions of the concept of "information legal relations" is performed, the author's definition of the concept of "information legal relations", their signs and features are presented.*

Keywords: *information, the right to information, information legal relations, proceedings, justice, protection of information legal relations.*

Аннотация. *Статья посвящена информационным правоотношениям как уникальному социальному явлению, их нормативному регулированию и охране. Несмотря на повышенный научный интерес, информационные правоотношения как юридическая категория, требуют дальнейшего исследования, поскольку сегодня существуют дискуссионные вопросы, которые еще не урегулированы законодателем. Систематизированы факторы, определяющие недостаточный уровень исследования информационных правоотношений на современном этапе, выполнен анализ научных определений понятия "информационные правоотношения", предлагается авторское понятие "информационные правоотношения", названы их признаки и особенности.*

Ключевые слова: *информация, право на информацию, информационные правоотношения, судопроизводство, правосудие, охрана информационных правоотношений.*

Постановка проблеми. В сучасних умовах стрімкого розвитку та становлення інформаційного права особливої уваги вимагають інформаційні правовідносини як унікальний вид суспільних відносин, об'єктом яких є інформація, а саме її створення, збирання, одержання, зберігання, використання, поширення, охорона та захист [1]. Унікальність інформаційних правовідносин визначається їх різноманітністю, оскільки інформаційними правовідносинами пронизані всі сфери сучасного суспільного життя. Як зазначає Д.О. Маріц, інформаційні правовідносини ми можемо розглядати у взаємозв'язку з іншими відносинами, які є у суспільстві [2, с. 64]. Слід зазначити, що інформаційні правовідносини потребують підвищеної уваги як науковців так і законодавця,

оскільки сьогодні існують певні методологічні та теоретичні положення, які мають дискусійний чи невизначений характер. В першу чергу залишається актуальною єдність нормативного визначення поняття "інформація" як юридичної категорії. Як відомо, поняття "інформація" застосовується в різних наукових сферах та тлумачиться в залежності від галузі використання, а тому має декілька значень. Для юридичної науки ця категорія має бути визначена однозначно, чого на даний час ще не зроблено, адже існують нормативно-правові акти, які вкладають в поняття "інформація" відмінний зміст.

Нормативне регулювання інформаційних відносин є необхідним, адже лише таким чином визначаються суб'єктивні права та юридичні обов'язки учасників правовідносин. Водночас, на нашу думку, дані правовідносини потребують не лише регулювання, але і охорони, яка має бути забезпечена відповідно до вимог законодавства України та положень міжнародних договорів, згода на обов'язковість яких надана Верховною Радою України.

Результати аналізу наукових публікацій. Протягом останніх років спостерігається підвищений науковий інтерес до проблем інформаційного права в цілому, та, зокрема, до сфери інформаційних правовідносин. Збільшується кількість публікацій, об'єктом дослідження яких є безпосередньо інформаційні правовідносини, а саме їх поняття, суб'єкти, об'єкт, зміст, підстави виникнення, зміни та припинення. Проблеми інформаційного права та інформаційних правовідносин в своїх дослідженнях представляють О.В. Арістова, О.А. Баранов, В.М. Боер, В.М. Брижко, Г.В. Виноградова, Л.П. Коваленко, В.А. Копилов, Б.А. Кормич, О.В. Кохановська, Д.О. Маріц, О.Г. Павельєва, В.Г. Пилипчук, О.П. Сидоренко, О.В. Синєокий, Р.В. Тарасенко, В.М. Фурашев та інші вчені.

Дослідження ґрунтується на працях з теорії держави і права, конституційного права, інформаційного права та цивільного процесуального права. Емпіричною базою дослідження національні нормативно-правові акти.

Метою статті є обґрунтування особливостей правового регулювання інформаційних відносин для їх охорони в судовому порядку.

Виклад основного матеріалу. Сучасне суспільство, без перебільшення, можна назвати інформаційним, тобто суспільством нового типу, в якому виникають, змінюються та припиняються інформаційні правовідносини. Ще до недавнього часу дану категорію правовідносин науковці в своїх дослідженнях обережно "оминали", що зрештою призвело до відсутності конкретизації в методології та теорії.

Правовідносини є об'єктом постійної уваги науковців, оскільки є явищем складним, багатогранним та мінливим. Водночас правовідносини є усталеною юридичною категорією, детально вивченою та розробленою. Таке подвійне становище означає, що дослідження правовідносин в різних аспектах має здійснюватися постійно. Як влучно зазначає О.І. Лятіна, безперешкодне співіснування та можливість вільного застосування при дослідженні правових відносин й соціальних явищ різних підходів сприяє як виявленню найширшого спектра ознак і властивостей цих відносин, так і встановленню об'єктивної і різносторонньої картини правового життя суспільства [3, с. 403]. Тому дослідження правовідносин в сучасних умовах потребує комплексного підходу, який враховує всі аспекти соціальних відносин.

Щодо інформаційних правовідносин, можемо виділити наступні чинники, які визначають недостатній рівень їх дослідження на сучасному етапі:

1) нормативно-правова база України досі не містить поняття інформаційних правовідносин, більше того, не визначає їх ознаки. На нашу думку слід розмежовувати

поняття “інформаційні правовідносини” та “інформаційні відносини”. У роботі [4, с. 11] наголошується, що інформаційні правовідносини виступають юридичною формою вираження та закріплення інформаційних відносин, які, у свою чергу, є формою певних публічних відносин. Інформаційні правовідносини є широким складним явищем, яке за свої змістом та ознаками є ширшим за поняття інформаційних відносин, які складаються виключно щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації.

Закон України “Про інформацію” в статті 2 називає основні принципи інформаційних відносин, до яких належать гарантованість права на інформацію, відкритість, доступність інформації, свобода обміну інформацією, достовірність і повнота інформації, свобода вираження поглядів і переконань, правомірність одержання, використання, поширення, зберігання та захисту інформації, захищеність особи від втручання в її особисте та сімейне життя. В статті 4 вказаного Закону встановлені суб’єкти інформаційних відносин, якими є фізичні особи, юридичні особи, об’єднання громадян, суб’єкти владних повноважень, а також визначений об’єкт інформаційних відносин, яким є інформація [1].

На наш погляд, така ситуація не означає “недопрацювання” законодавця, а свідчить про те, що інформаційні правовідносини як явище нове та таке, що стрімко розвивається, перебувають на стадії наукового розроблення. Завданням науковців на даному етапі є обґрунтування поняття, ознак, видів та основних характеристик інформаційних правовідносин як окремого виду відносин, що врегульовані правовими нормами;

2) спостерігається певна обережність окремих науковців у визначенні змісту інформаційних правовідносин, які для загальної теорії права є явищем новим та ще не вивченим на достатньому рівні. Як вже зазначалося, інформаційні правовідносини пронизують всі сфери суспільного життя, оскільки об’єктом таких відносин є інформація, або ж інформація щодо них стає предметом правого регулювання. Це не характеризує інформаційні правовідносини як похідні, тобто такі, які залежать від інших відносин, врегульованих нормами матеріального чи процесуального права. Навпаки, це підтверджує універсальність інформаційних правовідносин, що вимагає особливого комплексного підходу до їх дослідження;

3) інформаційні відносини поступово та стрімко “пронизують” всі сфери суспільного життя, в тому числі і такі, які, здавалося, давно усталені та врегульовані. Конституція України проголошує забезпечення інформаційної безпеки як одну із найважливіших функцій держави та справу всього українського народу (ч. 1 ст. 17); прямо забороняє такі дії як збирання, зберігання, використання або поширення конфіденційної інформації про особу без її згоди, окрім випадків, визначених законом, та виключно в інтересах національної безпеки, економічного добробуту та прав людини (ч. 2 ст. 32); гарантує кожному право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ч. 2 ст. 34). Водночас законодавець передбачає можливість обмеження законом здійснення цих прав 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 (ч. 5. ст. 34); судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім’ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (ч. 4 ст. 32);

гарантує кожному право вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення, причому така інформація ніким не може бути засекречена (ч. 2 ст. 50); відносить до кола питань, які визначаються виключно законами України, визначення засад утворення та діяльності засобів масової інформації (п. 11 ч. 1 ст. 92) [5].

Сучасні умови суспільного життя вимагають переоцінення підходів до розуміння сутності інформаційних правовідносин, до визначення їх суспільного значення та до розроблення механізмів їх правового регулювання. В цьому аспекті вбачаємо розвиток інформаційного права в напрямку від інформаційних відносин до інформаційних правовідносин, адже призначенням права є врегулювання суспільних відносин шляхом визначення суб'єктивних прав та юридичних обов'язків учасників правовідносин. І від того, наскільки таке правове регулювання буде ефективним та своєчасним, залежить як подальший розвиток правової науки, зокрема інформаційного права, так і загальний ефективний розвиток держави в напрямку демократичної, правової, суверенної і незалежної, соціальної інституції.

Сучасна юридична наука наразі неоднозначно визначає саму дефініцію "інформаційні правовідносини". Протягом останніх років здійснено ряд наукових досліджень щодо визначення поняття інформаційних правовідносин. У загальному розумінні інформаційні правовідносини визначаються як "врегульовані інформаційно-правовою нормою інформаційні відносини, сторони яких виступають в якості носіїв взаємних прав та обов'язків, встановлених та гарантованих інформаційно-правовою нормою" [6, с. 122]. О.В. Синєокий стверджує, що інформаційні правовідносини – це суспільні відносини, які виникають під час створення, розподілу та використання інформації та врегульовані нормами інформаційного права, учасники якого володіють відповідними юридичними правами та обов'язками [7, с. 98]. Д.О. Маріц пропонує оперувати категорією "інформаційні відносини", яка охоплює відносини, які регулюються нормами публічного та приватного права, які виникають між суб'єктами суспільних відносин на підставі юридичних фактів [2, с. 67]. М.В. Фігель визначає інформаційні правовідносини як урегульовані нормами інформаційного права суспільні відносини, учасники яких виступають носіями юридичних прав і обов'язків, що регулюють приписи щодо створення, розподілу та використання інформації, які містяться в цих нормах [8, с. 234]. Л.П. Коваленко доходить висновку, що інформаційні правовідносини – це юридична форма вираження інформаційних відносин, коли останні можуть існувати виключно в правовій формі [9, с. 4].

На основі аналізу низки наукових праць, присвячених дослідженню інформаційних правовідносин, та керуючись загальними принципами інформаційного права, пропонуємо авторське визначення інформаційних правовідносин як відносин, що врегульовані нормами права, які виникають між різними суб'єктами щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та охороняються державою від порушень.

Виконавши дослідження, складно погодитися з висновком Л.П. Коваленко, що інформаційні відносини характеризуються певним похідним характером [9, с. 1]. Інформаційні правовідносини є окремим видом суспільних відносин, врегульованих правовими нормами. На наш погляд інформаційним правовідносинам властиві певні особливості, які вирізняють їх серед інших правовідносин:

1) *предмет регулювання*: законодавство України регулює відносини, які складаються щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації Згідно ч. 1 ст. 1 Закону України "Про інформацію" інформацією є

будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [1]. В ч. 1 ст. 1 Закону України "Про телекомунікації" інформація вже трактується як відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [10]. Цивільний кодекс України відносить інформацію до нематеріальних благ та визначає як будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді [11].

Б.А. Кормич, узагальнюючи нормативні визначення інформації, визначає інформацію як відомості, що були організовані в такій формі, документовані, передані або оголошені таким чином, що можуть бути сприйнятими іншою особою [12, с. 10]. Складно не погодитися з думкою В.Г. Пилипчука щодо того, що відсутність єдності в розумінні сутності інформації як ключової складової інформаційного суспільства та світового інформаційного простору становить системну проблему [13, с. 17]. Німецький вчений Вернер Гітт, дослідивши сутність інформації, дійшов висновку, що інформація – це третя фундаментальна величина, що існує поряд з енергією та матерією, які з давніх часів вважаються основоположними та універсальними величинами будь-якої галузі науки та техніки. Інформація по своїй сутності є такою ж широкою та фундаментальною величиною [14]. Як визначає В. Пилипчук, подібних висновків дійшли ще ряд провідних вчених, які також виділяють інформацію як окрему фундаментальну величину, яка не є ні матерією, ні енергією [13, с. 17].

У загальному розумінні термін "інформація" походить від латинського слова "informatio", яке має кілька значень: роз'яснення, виклад фактів, подій, витлумачення, представлення, поняття, ознайомлення, просвіта [15]. Досі існує складність у визначенні єдиного значення цього терміну, оскільки ним оперують в багатьох сферах людської діяльності, а тому використання даного терміну в різних значеннях є цілком зрозумілим. Що ж до юриспруденції, яка має на меті встановлення правопорядку та законності, то нормативне закріплення розуміння інформації як фундаментальної категорії є необхідним.

В цьому аспекті хочемо акцентувати увагу на тому, що Цивільний кодекс України виокремлює інформацію серед інших нематеріальних благ, до яких відносить а) результати інтелектуальної, творчої діяльності, б) особисті немайнові блага та в) інформацію. Причому в ч. 3 ст. 200 вказується, що порядок використання інформації та захисту права на неї встановлюється законом [11]. Додатково Закон України "Про доступ до публічної інформації" регулює відносини, які виникають щодо окремого виду інформації – *публічної інформації*, тобто такої, що знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених Законом, та інформації, що становить суспільний інтерес. В статті 1 Закону публічна інформація визначена як відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом [16]. Також нормативно окремо визначається публічна інформація з обмеженим доступом, до якої належить: 1) конфіденційна інформація; 2) таємна інформація; 3) службова інформація. Обмеження доступу до інформації здійснюється відповідно до Закону, виключно 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, якщо

розголошення інформації може завдати істотної шкоди вказаним інтересам та шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні. Водночас не може бути з обмеженим доступом інформація щодо розпорядження бюджетними коштами, володіння, користування чи розпорядження державним, комунальним майном, у тому числі копії відповідних документів, умови отримання цих коштів чи майна, прізвища, імена, по батькові фізичних осіб та найменування юридичних осіб, які отримали ці кошти або майно. При дотриманні вимог, передбачених частиною другою статті 6, зазначене положення не поширюється на випадки, коли оприлюднення або надання такої інформації загрожує завданням шкоди інтересам національної безпеки, оборони, розслідуванню чи запобіганню злочину. Конфіденційна інформація визначається як така, 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. Законодавець чітко встановлює перелік відомостей, які не можуть бути віднесені до конфіденційної інформації, зокрема про стан довкілля, про якість харчових продуктів і предметів побуту, про аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статися і загрожують здоров'ю та безпеці громадян, а також інша інформація, що становить суспільний інтерес (суспільно необхідна інформація), зазначена в частині першій і другій статті 13 цього Закону. Розпорядники, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини. Таємною визначається інформація, доступ до якої обмежується та розголошення якої може завдати шкоди особі, суспільству і державі. Таємною може визнаватися інформація, яка містить державну, професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю. До службової інформації можуть відноситися наступні дані: 1) які містяться в документах суб'єктів владних повноважень та становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень; 2) які зібрані в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни та які не віднесено до державної таємниці. Документам, що містять інформацію, яка становить службову інформацію, присвоюється гриф "для службового користування". Доступ до таких документів обмежується та надається відповідно до частини другої статті 6 Закону [16];

2) *універсальність*: інформаційні правовідносини присутні у всіх соціальних сферах, у кожній галузі права. Т.А. Костецька зазначає, що інформаційні правовідносини знаходяться у сфері впливу держави як відносини, що виникають у процесі інформаційної діяльності суспільства, держави, засобів масової інформації в інформаційній сфері [17, с. 64]. Оскільки інформаційна діяльність суспільства є невід'ємним атрибутом його функціонування, можемо дійти висновку, що інформаційні відносини присутні в нашому сьогоденні постійно.

В сучасних умовах інформація є невід'ємним атрибутом життєдіяльності суспільства, а це означає, що відносини, які виникають у зв'язку з її створенням, збиранням, одержанням, зберіганням, використанням, поширенням та захистом, потребують не тільки нормативного регулювання щодо застосування, але й щодо їх охорони, оскільки створення належного механізму захисту прав, в тому числі права на

інформацію, є одним із завдань державного управління. Вважаємо доцільним акцентувати увагу безпосередньо на проблемі охорони інформаційних правовідносин, яка може забезпечуватися в судовому порядку. Конституція України в статті 55 однозначно проголошує, що права та свободи людини і громадянина захищаються судом і кожному гарантується право оскаржити в суді рішення, дії чи бездіяльність органів державної влади, органів місцевого самоврядування, посадових і службових осіб. Виключно суди здійснюють правосуддя в Україні, а юрисдикція суду поширюється на будь-який юридичний спір та будь-яке кримінальне обвинувачення (ст. 124) [5]. В Україні гарантується право кожного на справедливий суд [18].

Право на інформацію, відображене в статті 5 Закону України "Про інформацію" означає право кожного мати можливість вільно одержувати, використовувати, поширювати, зберігати та захищати інформацію, необхідну для реалізації своїх прав, свобод і законних інтересів. Водночас, реалізація права на інформацію не повинна здійснюватися всупереч громадським, політичним, економічним, соціальним, духовним, екологічним та іншим правам, свободам і законним інтересам інших громадян, а також правам та інтересам юридичних осіб. Не допускається зловживання правом на інформацію, що означає те, що інформація не може використовуватися для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини (ст. 28) [1].

Інформаційні правовідносини потребують особливої уваги в аспекті їх охорони, зважаючи на властивості предмету правового регулювання, про що вже зазначалося раніше. Значне місце в механізмі захисту інформаційних правовідносин займає цивільне судочинство, завданням якого є справедливий, неупереджений та своєчасний розгляд і вирішення цивільних справ з метою ефективного захисту порушених, невизнаних або оспорюваних прав, свобод чи інтересів фізичних осіб, прав та інтересів юридичних осіб, інтересів держави. Але слід зазначити, що при відправленні цивільного судочинства також складаються правовідносини, які можна кваліфікувати як інформаційні. Так стаття 8 ЦПК України проголошує відкритість інформації щодо цивільної справи, що унеможливлює позбавлення особи права на визначену інформацію, а саме про дату, час і місце розгляду своєї справи. Окрім того, ніхто не може бути обмежений у праві отримання в суді усної, письмової інформації про результати розгляду його судової справи. У порядку, встановленому Законом, будь-яка особа, яка не є учасником справи, має право на доступ до судових рішень [19].

Закон України "Про доступ до судових рішень" в статті 2 проголошує, що всі судові рішення є відкритими та підлягають оприлюдненню в електронній формі не пізніше наступного дня після їх виготовлення і підписання [20]. З метою забезпечення загального доступу до судових рішень Державна судова адміністрація України здійснює ведення Єдиного державного реєстру судових рішень (далі – ЄДРСР) [21]. ЄДРСР – це автоматизована система збирання, зберігання, захисту, обліку, пошуку та надання електронних копій судових рішень. ЄДРСР є державною інформаційною системою, що входить до складу Єдиної судової інформаційної системи і забезпечує збирання, облік (реєстрацію), накопичення, зберігання, захист, пошук та перегляд інформаційних ресурсів Реєстру та їх образів [22]. Слід зазначити, що в ЄДРСР відображається не вся інформація щодо справи, зокрема не відображається інформація, яка за рішенням суду щодо розгляду справи у закритому судовому засіданні підлягає захисту від розголошення при судовому розгляді у закритому судовому засіданні. ЄДРСР є

відкритим для безоплатного цілодобового доступу на офіційному веб-порталі судової влади України.

Закон України "Про доступ до публічної інформації" регулює порядок доступу до інформації, який може здійснюватися в два шляхи: 1) шляхом систематичного та оперативного оприлюднення інформації в офіційних друкованих виданнях ,на офіційних веб-сайтах в мережі Інтернет, на єдиному державному веб-порталі відкритих даних, а також на інформаційних стендах та будь-яким іншим способом; 2) шляхом надання інформації за запитами на інформацію [16]. Так за даними, викладеними Вищою радою правосуддя у "Звіті про виконання Закону України "Про доступ до публічної інформації" у 2018 році" за звітний період до ВРП на розгляд надійшло 772 запити на інформацію. Запити на інформацію надійшли: від фізичних осіб – 648 (електронною поштою – 416, поштою – 169, подано особисто запитувачами – 43, телефоном – 20); від представників засобів масової інформації – 52 (електронною поштою – 39, поштою – 11, подано особисто представниками – 2); від юридичних осіб – 17 (електронною поштою – 7, поштою – 9, подано особисто представником – 1); від об'єднань громадян (громадських організацій) – 55 (електронною поштою – 14, поштою – 30, особисто представниками громадської організації – 11).

Цікавим є зміст інформації, яка була надана ВРП на запити, зокрема: інформація з питань діяльності Вищої ради правосуддя та секретаріату Ради; внесення Президентові України подань про призначення суддів на посади; перебування на розгляді Ради подань Вищої кваліфікаційної комісії суддів України щодо відрядження суддів, як тимчасового переведення до інших судів того самого рівня і спеціалізації; щодо кількості поданих суддями заяв про відставку або про звільнення з посади за власним бажанням та звільнених з даних посад за відповідний період; відомостей про кількість подань Генеральної прокуратури України та прийнятих Радою рішень про надання згоди на застосування до суддів запобіжного заходу у виді утримання під вартою, а також тимчасове відсторонення суддів у зв'язку з притягненням до кримінальної відповідальності; інформації щодо кількості висновків і скарг, переданих Тимчасовою спеціальною комісією з перевірки суддів судів загальної юрисдикції до Вищої ради юстиції та результатів їх розгляду Вищою радою юстиції (правосуддя); господарської діяльності Вищої ради правосуддя тощо [23].

Висновки.

З огляду на вищезазначене можемо підсумувати:

1) інформаційні правовідносини є унікальним видом суспільних відносин, врегульованих нормами права, оскільки присутні у всіх сферах суспільного життя та мають комплексний характер. Інформаційні правовідносини можемо розглядати у взаємозв'язку з іншими відносинами, які є у суспільстві [2, с. 64];

2) інформаційні правовідносини – це суспільні відносини, що врегульовані нормами права, які виникають між різними суб'єктами щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації та охороняються державою від порушень;

3) інформаційні відносини потребують не тільки нормативного регулювання, але і охорони, забезпечення якої є можливим в судовому порядку. Право на інформацію закріплене нормативно, водночас його реалізація не повинна здійснюватися всупереч громадським, політичним, економічним, соціальним, духовним, екологічним та іншим правам, свободам і законним інтересам інших громадян, правам та інтересам юридичних осіб, а також інтересам держави.

Використана література

1. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.

2. Маріц Д.О. Поняття та зміст інформаційних правовідносин. *Jurnalul juridic national: teorie şipractică.* 2016. № 5. С. 64-67.

3. Лятіна О.І. Поняття правовідносин у контексті законницької та юридичної доктрин. *Часопис Київського університету права*. 2013. № 4. С. 403-406.

4. Цимбалюк В.С. Інформаційне право: визначення сутності та змісту як комплексної галузі права. *Правова інформатика*. 2005. № 2. С. 5-14.

5. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

6. Копилов В.А. Информационное право: учебник. Изд. 2-е, перераб. и доп. Москва: Юрист, 2002. 512 с.

7. Синєокий О.В. Високотехнологічне інформаційне право України. Харків: Право, 2010. С. 360.

8. Фігель М.В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. С. 336.

9. Коваленко Л.П. Інформаційні відносини. URL: file:///C:/Users/Ira/Downloads/62395-128225-1-SM%20(2).pdf (дата звернення 21.11.2019).

10. Про телекомунікації: Закон України від 18.11.03 р. № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

11. Цивільний кодекс України: Закон України від 16.01.03 р. *Відомості Верховної Ради України.* 2003. №№ 40-44. Ст. 356.

12. Кормич Б.А. Інформаційне право: підручник. Харків: БУРУН і К., 2011. С. 334.

13. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері. *Вісник Академії правових наук України*. 2011. № 3. С. 16-27.

14. Вернер Гитт. Информация: третья фундаментальная величина. URL: http://scienceandapologetics.com/stati/426-informaciya-tretya-fundamentalnaya-velichina.html (дата звернення 21.11.2019).

15. Інформація. URL: https://uk.wikipedia.org/wiki/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F (дата звернення 21.11.2019).

16. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.

17. Костецька Т.А. Актуальні проблеми державно-правового регулювання інформаційних відносин. *Часопис Київського університету права*. 2006. № 4. С. 63-68.

18. Про судоустрій і статус суддів: Закон України від 02.06.16 р. № 1402-VIII. *Відомості Верховної Ради*. 2016. № 31. Ст. 545.

19. Цивільний процесуальний кодекс України: Закон України від 18.03.04 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст.492.

20. Про доступ до судових рішень: Закон України від 22.12.05 р. № 3262-IV. *Відомості Верховної Ради України*. 2006. № 15 Ст. 128.

21. Єдиний державний реєстр судових рішень. *Судова влада України.* URL: http://reyestr.court.gov.ua (дата звернення 27.11.2019).

22. Порядок ведення Єдиного державного реєстру судових рішень: рішення Вищої ради правосуддя від 19.04.18 р. № 1200/0/15-18. URL: http://www.vru.gov.ua/act/14049 (дата звернення 27.11.2019).

23. Про виконання Вищою радою правосуддя Закону України "Про доступ до публічної інформації" у 2018 році: звіт від 04.01.19 р. *Вища рада правосуддя.* URL: http://www.vru.gov.ua/statistics/94 (дата звернення 25.11.2019).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.7

ГОЛОВКО О.М., *кандидат юридичних наук,* старший науковий співробітник НДІ інформатики і права НАПрН України, старший викладач кафедри публічного права Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

ЦИФРОВА КУЛЬТУРА ТА ІНФОРМАЦІЙНА КУЛЬТУРА: ПРАВА ЛЮДИНИ В ЕПОХУ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Анотація. *Продемонстровано, що процес цифровізації викликає численні питання регулювання правовідносин, пов'язаних з ним, а також формує нові напрями забезпечення прав людини. Встановлено, що відсутність єдиної термінології, зокрема, щодо інформаційної та цифрової культур нівелює розуміння можливостей, а отже й прав, що виникають або зазнають модифікації внаслідок цифрових трансформацій.*

Ключові слова: *цифровізація, права людини, цифрові права, цифрова культура, інформаційна культура.*

Summary: *It has been demonstrated that the digitalisation raises numerous issues of regulation of legal relationships associated with it, and also forms new directions for human rights. It is established that the lack of common terminology, in particular regarding information and digital cultures, makes it impossible to understand the possibilities and therefore the rights that arise or get modifications as a result of digital transformations.*

Keywords: *digitalization, human rights, digital rights, digital culture, information culture.*

Аннотация. *Продемонстрировано, что процесс цифровизации вызывает многочисленные вопросы регулирования правоотношений, связанных с ним, а также формирует новые направления обеспечения прав человека. Установлено, что отсутствие единой терминологии, в частности, информационной и цифровой культур делает нивелирует понимание возможностей, а следовательно и прав, возникающих или испытывающих модификации вследствие цифровых преобразований.*

Ключевые слова: *цифровизация, права человека, цифровые права, цифровая культура, информационная культура.*

Постановка проблеми. Необхідність осмислення процесів цифровізації пов'язана з багатьма соціальними та правовими змінами, яких потребує суспільство задля стабільності та безпеки. Інформаційна культура населення є запорукою цього. Усвідомлений підхід до епохи цифрових трансформацій потребує від держави нового бачення цифрової культури та цифрових прав людини, адже саме вони покладені в основу превенції загроз в інформаційному просторі. Термінологічна неузгодженість вище окреслених понять, законодавча невизначеність у їх співвідношенні спотворює механізм правого регулювання нових (цифрових) модифікацій вже існуючих (інформаційних) правовідносин.

Результати аналізу наукових публікацій. Теоретичною основою цієї роботи є національні та міжнародні нормативно-правові акти, а також погляди на інформаційну культуру та права людини таких вчених, як Бенедек Ф., Бєляков К., Венгеров А., Головистикова А., Грудцина Л., Дзьобань О., Долуда В., Золотар О., Кеттеман М., Маляренко Т., Мануйлов Є.М., Онупрієнко С., Панченко О.А., Панченко Л., Шебаніц Д., Шопіна І. та ін.

Метою статті є визначення взаємозв'язку інформаційної культури та цифрової культури, а також з урахуванням отриманих результатів здійснення спроби виокремити перелік цифрових прав людини в епоху цифрових трансформацій.

Виклад основного матеріалу. Нещодавні трансформації соціального середовища, поява нових прав людини, що випливають з раніше виокремлених або кардинально нові права, котрі науковці часто відносять до четвертого покоління прав людини зумовлюють потребу в чіткому визначенні їх сутності та кореляції з основоположними правами людини в усталеній парадигмі Human Rights.

На відміну від традиційних підходів до аналізу змісту і сутності прав людини пропонуємо розглядати їх через призму понять "інформаційна культура" та "цифрова культура", адже саме підвищення їх рівня, судячи з національного законодавства, має створити умови для забезпечення інформаційної безпеки людини.

Ця думка підтверджується багатьма вченими. Дзьобань О.П. наголошує, що рівень інформаційної культури суб'єкта прямо пропорційний рівню інформаційної безпеки і, причому, що вище рівень інформаційної культури – то менше загроз останньої (тобто то вище рівень інформаційної безпеки) [1, с. 77]. Золотар О.О. визначає те, що можливості реалізації прав і свобод людини суттєво залежать від адаптованості до них самої особи, інститутів суспільства і держави, а також системи права, що першочергово зумовлено високим ступенем інформаційної та правової культури [2, с. 64].

Пропонуємо розглянути понятійно-категоріальний апарат, який існує в правовому полі України щодо окреслених понять, та встановити співвідношення між ними.

Розпорядженням Кабінету Міністрів України "Про схвалення Стратегії розвитку інформаційного суспільства в Україні" від 15.05.2013 р. № 386-р. було введено поняття "електронна культура". Це форма культури, яка передбачає стимулювання та мотивування поширення здобутків у сфері культури за допомогою інформаційно-комунікаційних технологій (далі – е-культура). Як випливає з даного визначення, електронна культура передбачає наявність навичок поширення досягнень культури в інформаційному просторі. Можливість поширення інформації включається в право на інформацію як невід'ємний її компонент, з чого випливає, що електронна культура є вужчим поняттям, аніж інформаційна культура, визначення якої в законодавстві критично не вистачає.

Актуалізація явища інформаційної культури відбулася на етапі реалізації інформаційних загроз в результаті відкритої зовнішньої агресії, спрямованої на інформаційну безпеку держави. В цей період спостерігається підвищений інтерес до інформаційної культури населення. Результатом діяльності законодавця є Доктрина інформаційної безпеки України, затверджена Указом Президента України від 25 лютого 2017 р. № 47/2017. В ній надано таке поняття як "медіа-культура". Однак, визначення даному поняттю знову не надано законодавцем, що унеможливлює єдине трактування та кореляцію з суміжною термінологією. Окрім цього, ускладнюється реалізація визначеного Доктриною такого національного інтересу України в інформаційній сфері як розвиток медіа-культури суспільства та соціально відповідального медіа-середовища.

Наразі в Україні та світі активно обговорюються зміни в юридичній науці та практиці у зв'язку з так званою цифровою трансформацією суспільства. Українська влада, залишаючись в тренді цих змін, усіляко сприяє процесу трансформації, результатом чого станом на сьогодні ми маємо розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та затвердження плану заходів щодо її реалізації" від 17 січня 2018 р. № 67 (далі – Концепція).

Серед основних цілей цифрового розвитку Концепцією визначено, зокрема, розвиток та поглиблення цифрової компетенції громадян для забезпечення їх готовності до використання цифрових можливостей, а також подолання супутніх ризиків. Концепція передбачає здійснення заходів щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрової компетенції, а також визначає критичні сфери та проекти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій.

Зі змісту Концепції випливає, що цифрові компетенції – це уміння використовувати цифрові технології, ключову роль з яких надають цифровій грамотності. Як зазначають деякі вчені, обізнаність щодо можливостей використання Інтернету (“цифрова грамотність”) – це передумова здатності здійснювати свободу вираження поглядів он-лайн [3, с. 43].

Таким чином, з’являються ще поняття “цифрові компетенції” та “цифрові можливості”, які так само співвідносяться з вищезгаданими поняттями виключно на власний розсуд. Очевидно, що наявність цифрової грамотності передбачає формування цифрової культури особи.

Результатом аналізу тільки декількох документів маємо абсолютну неузгодженість термінології та перелік таких понять як “електронна культура”, “медіа-культура” та “цифрова культура”, які за попередньою оцінкою можна об’єднати в єдине ціле – інформаційну культуру.

Для стабільного становища людини в суспільстві слід підкреслити важливість утворення інформаційних зв’язків, які виступають як спосіб організації інформаційного простору, інформаційного поля індивіда. Ці аспекти сприяють формуванню інформаційної культури суспільства та індивідуальної інформаційної культури [4]. В. Долуда наголошує, що цінності європейської демократії просто не могли б бути реалізованими, якби корелятом їх становлення не виступала інформаційна культура, традиції якої перетворилися на важливу складову суспільного життя західних держав. У сучасних демократичних країнах інформаційні технології є невід’ємною складовою їх політичної культури з чітко розмежованими функціями держави та громадянського суспільства, а обмеження на володіння інформацією регламентуються як законами, так і нормами звичаєвого права [5].

Поняття “інформаційна культура” містить в собі узагальнення, які стосуються інформаційних знань, умінь і навичок людини, її здатності працювати з інформацією тощо [6]. Під інформаційною культурою особистості розуміється властивість особистості, що характеризує її як суб’єкта інформаційної діяльності і визначає відношення до функціонування і розвитку інформаційної сфери суспільства [7].

Процес формування інформаційної культури покликаний ліквідувати значні проблеми сьогодення, на яких наголошують науковці. Так, серед головних проблем, які характеризують ситуацію в національній культурній та інформаційній сферах сучасної України, дослідники виділяють “культурний шок”, зумовлений зіткненням різних способів життя, систем цінностей (а отже, й різних культур) у процесі суспільних трансформацій [8, с. 373]. Одним із напрямів розвитку інформаційної культури є формування навичок для захисту від інформаційного стресу, який багато в чому породжується дисбалансом між зростаючим потоком інформації і здатністю суб’єкта (людини, суспільства) до її обробки [9, с. 165]. Для значної частини користувачів (особливо для представників молодого покоління) Інтернет постає насамперед сферою

розваг (комп'ютерних ігор, віртуального спілкування), що не свідчить про високий рівень існуючої інформаційної культури [10, с. 20].

Розглядаючи поняття цифрової культури, варто звернутися до визначеного в Концепції процесу цифровізації, як насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможливлює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір.

Виникає логічне запитання, що включає в себе поняття "кіберфізичний простір", адже надання визначення поняттю в законодавстві має спрощувати, а не ускладнювати розуміння сутності правовідносин, які потребують врегулювання через соціальні, культурні чи будь-які інші зміни.

Провідні науковці вже давно наголошують на наявності плутанини в термінології, пов'язаної з аспектами підвищення інформаційної культури. Одночасне існування у національному законодавстві термінів "електронна культура", "мережева культура", "віртуальна культура", "кіберкультура", "медіа-культура", "медіа-грамотність", "комп'ютерна грамотність", "цифрова грамотність", "інформаційно-комп'ютерна грамотність", "комп'ютерна вправність", "інформаційно-комунікативна компетентність", "культура безпекового поводження в кіберпросторі" не дають змоги побудувати ефективну систему розвитку інформаційної культури [11, с. 109]. З даним твердженням важко не погодитися, адже воно вказує на комплексність поняття інформаційної культури, яке потребує усунення безсистемного підходу законодавця. Це, в свою чергу, створить умови для підвищення рівня інформаційної культури суспільства та забезпечення прав людини в повному обсязі з урахуванням мінливості інформаційного простору та стрімкого розвитку інформаційно-комп'ютерних технологій (далі – ІКТ).

Цікавою видається культура інформаційної безпеки як спосіб організації і розвитку інформаційного суспільства, що забезпечує якісне інформаційне середовище (якість споживаної інформації, захищеність суб'єкта від негативних інформаційних дій), створює можливість повністю задовольнити інформаційні потреби суб'єкта, і при якому він усвідомлює себе суб'єктом інформаційної безпеки, здатний виявити загрози, володіє технологіями захисту від них, дотримується норм інформаційної етики в процесі перетворення інформаційного середовища [12, с. 37].

Повертаючись до аналізу процесу цифровізації, зазначимо, що відповідно до п. 3 Положення про Міністерство цифрової трансформації України (далі – Положення), затвердженого постановою Кабінету Міністрів України від 18 вересня 2019 р. № 856, існує чіткий перелік сфер реалізації діяльності Міністерства, а отже визначено напрями державної політики, пов'язані з процесами цифровізації. Питання розвитку цифрових навичок та цифрових прав громадян об'єднано в одну сферу, що вказує на комплексний підхід держави. Створення державою умов для забезпечення громадянам можливості розвитку своїх цифрових навичок, з одного боку, та формування правового підґрунтя для реалізації комплексу цифрових прав є запорукою успіху цифровізації в державі.

Загалом, на рівень інформаційної культури людини, яка, на нашу думку, включає аспекти розвитку цифрових навичок, впливають численні фактори, серед яких окрему увагу варто приділяти питанням забезпечення цифрових прав людини.

Однак на даному етапі постає основне питання: якщо йде мова про термінологічну неузгодженість між інформаційною та цифровою культурою як основи забезпечення безпеки людини в інформаційній сфері, яким чином можливе виокремлення її цифрових прав? Для цього необхідно усвідомити, що інформаційні права та цифрові права співвідносяться як ціле і частина.

Варто зазначити, що про інформаційні права в чистому вигляді людство заговорило відносно нещодавно, адже вони вважаються правами четвертого покоління прав людства, на чому наголошує А.Б. Венгеров [13, с. 307]. На відміну від А.Б. Венгерова, деякі вчені до четвертого покоління прав зараховують виключно інформаційні права та технології [14, с. 125]. Д.М. Шебаніц серед прав четвертого покоління виокремлює право на використання віртуальної інформації [15, с. 59]. Ці права ще часто виокремлюють в комплекс віртуальних прав.

Як зазначає Маляренко Т., безпека людини і права людини є тісно пов'язаними. Вона базується на забезпеченні прав людини, а також враховує права людини "третього покоління", в тому числі право на розвиток і право на мир [16, с. 17]. В попередніх дослідженнях нами було запропоновано виділити право людини на інформаційну безпеку як одне з прав так званого "четвертого покоління". В нашому дослідженні йшлося про безпеку саме у віртуальному середовищі. Втім, як бути з тими інформаційними правами та свободами, які з'явилися в так званий доцифровий період?

Яскравим прикладом таких інформаційних прав є ст. 12 Загальної декларації прав людини (далі – Декларація), яка виокремлює свободу від втручання в особисте і сімейне життя, від посягання на недоторканність житла, таємницю кореспонденції. Очевидно, що в частині про таємницю кореспонденції є чітко виражене право на приватність. Якщо повернутись до класифікатора прав людини за історичними поколіннями варто зазначити, що Декларація була рушієм формування другого покоління прав людини. Це призводить до думки про тісний взаємозв'язок всіх виокремлених поколінь прав людини та навіть ставить питання про доцільність такого поділу. Втім, цей аспект може стати предметом окремих досліджень.

Наступні покоління прав людини часто базуються на попередніх, виносячи на перший план нагальні потреби суспільства. Узагальнюючи сутність поділу прав людини на покоління, зазначимо, що перше покоління прав людини сформувалося на основі впровадження ідеї рівності всіх перед законом, що передбачає рівні права будь-якої людини незалежно від раси, статі, кольору шкіри тощо, тобто такі, що людина має від народження (негативні права); друге покоління прав людини базується на формуванні соціальних, економічних та культурних прав, реалізація яких неможлива без організаційно-правового забезпечення їх реалізації з боку держави (позитивні права); третє покоління включає в себе ті права, реалізація яких передбачає гуманістичний підхід до людини в цілому, адже ці права розглядаються через призму прав націй, народів, певного соціального осередку, людства в цілому; четверте покоління пов'язане з певними науковими відкриттями та дослідженнями тих можливостей, яких досі людство не мало.

Останнє стосується багатьох сфер життя людини, однак в інформаційній сфері такі права часто пов'язують із появою Інтернету, розвитком ІКТ загалом, появою кардинально нових пристроїв для реалізації своїх потреб, наприклад, технології Інтернету речей (IoT). Інноваційність технологій викликає закономірні питання щодо правового регулювання таких правовідносин, потреби зміни та/або вдосконалення механізмів забезпечення прав людини, а також виділення нових, які також можуть виступати об'єктом захисту.

Українському законодавцю також відомі певні новели, пов'язані з правами людини у Всесвітній мережі. Так, проектом Закону України "Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету)", запропоновано доповнити ст. 302 ЦК такими рядками: "Фізична особа має право на доступ до Інтернету. Право фізичної особи на доступ до Інтернету не може

бути обмежене. Обмеження доступу до певних даних, що містяться у Інтернеті, можливо лише на підставі рішення суду про незаконність таких даних" [17].

Резолюцією Парламентської асамблеї Ради Європи 1877 (2012) було закріплено свободу слова та інформації в Інтернеті та он-лайн ЗМІ [18]. Здається, що мова йде про вже відому юристам конструкцію "свобода слова", однак з появою Інтернету виникли складнощі в реалізації даної свободи у віртуальному просторі, що змушує виділяти певні права та свободи, які є похідними від вже існуючих.

Деякі дослідники вирізняють такі права і свободи як вільний доступ до Інтернету, свобода слова у Всесвітовій мережі, вільний доступ до інформації через Інтернет. Таким чином, спостерігаємо деталізацію та розгалуження вже відомих у світі прав та свобод людини на такі, які пов'язані саме з процесом цифровізації. Більш вдалою видається пропозиція про виділення суміжних прав, таких як свобода зібрань та об'єднань он-лайн, право на (цифрову) освіту та доступ до цифрових знань [3, с. 41]. Така класифікація одразу вказує на сегментування відомих людству прав людини на такі, що пов'язані з віртуальним простором.

На нашу думку, права людини варто розглядати через призму можливостей та компетенцій, реалізація яких має забезпечуватися державою. Пропонуємо застосувати цей підхід при аналізі Рекомендації 2006/962/ЄС Європейського Парламенту та Ради (ЄС) "Про основні компетенції для навчання протягом усього життя", які уособлюють високий рівень інформаційної культури. В даному акті передбачено компетенції, необхідні для роботи з цифровими носіями. Серед них можна виділити такі:

1) використання комп'ютерів для електронної обробки тексту, електронних таблиць, баз даних, зберігання та керування інформацією;

2) розуміння можливостей та потенційних небезпек Інтернету і спілкування за допомогою електронних засобів масової інформації та цифрових технологій;

3) розбиратись у достовірності та надійності доступної інформації, що можливе, в тому числі, за рахунок інформації та інструментів зі Всесвітньої мережі;

4) здатність до пошуку, збирання та обробки інформації, критичного та систематичного її використання, оцінки її значимості;

5) здатність розрізняти реальність від віртуальної реальності, при вмінні їй пов'язати;

6) бути здатними отримати доступ, знайти та скористатись послугами Інтернет-служб тощо.

Розглядаючи роль доступу до Інтернету радше як каталізатор для інших прав людини та сприяння змінам, існують пропозиції запровадити підхід до розмежування доступу до Інтернет-контенту та фізичного доступу через наявну інфраструктуру [19].

Подібні підходи наполягають скоріше на важливості цифровізації та її потенціалу щодо забезпечення комплексу прав людини загалом, тобто як інструмент забезпечення, а не простір, для захисту прав людини в якому потребується виділення спеціального комплексу прав.

Численні пропозиції щодо виділення нового комплексу цифрових прав та його потенції до внесення в четверте покоління прав людини безперечно наявні. Втім, успіх даної справи можливий тільки за рахунок термінологічної узгодженості законодавства, пов'язаного з цифровізацією з урахуванням європейської практики.

Висновки.

Термінологічна неузгодженість між інформаційною та цифровою культурою як основами забезпечення безпеки людини в інформаційному просторі, ускладнює реалізацію можливостей, які надає людині епоха цифрових трансформацій.

Взаємозв'язок інформаційної та цифрової культури є очевидним, а компетенції, що вони передбачають, дають можливість реалізовувати право на (цифрову) інформацію, право на доступ до Інтернету, право на (цифрову) освіту тощо. Інформаційні та цифрові права співвідносяться як ціле і частина, що зумовлює певну плутанину в правовому полі. Наразі більшість цифрових прав є похідними від інформаційних та відображають сутність реалізації тих компетенцій, що має людина з високим рівнем інформаційної культури. Однак, епоха цифрових трансформацій спричинює формування нового наукового дискурсу, який веде до думки про появу нових прав, таких як право на використання віртуальної реальності, право на доступ до Інтернет (право на цифровий доступ), право на доступ до цифрових знань та цифрової освіти тощо.

Використана література

1. Дзьобань О.П., Мануйлов Є.М. Інформаційна безпека в контексті інформаційної культури. *Інформація і право*. № 1(20)/2017. С. 74-81.

2. Золотар О.О. Права і свободи людини: інформаційний вимір: зб. мат. наук.-прак. конф. *ІТ право: проблеми і перспективи розвитку в Україні,* м. Львів, 18 лист. 2016 р. Львів, 2016. С. 59-68.

3. Бенедек Ф., Кеттеман М. Свобода вираження поглядів та Інтернет. П.: Видавництво Ради Європи, 2013. 204 с.

4. Дзьобань О. П., Жданенко С. Б. Інформаційна культура: до питання про основні етапи розвитку. *Політологічний вісник*. 2015. Вип. 77. С. 353-365.

5. Долуда В.В. До питання про формування національної інформаційної інфраструктури. URL: http://archive.nbuv.gov.ua/portal/Soc_Gum/Gileya/2011_45/Gileya45/P8_doc.pdf

6. Калиновская Н.А. Информационный стресс. Информационно-психологическая безопасность личности как качественная характеристика информационной культуры человека: монография. URL: http://www.twirpx.com/file/ 354820.

7. Алиева М.Ф. Информационная безопасность как элемент информационной культуры. *Вестник Адыгейского государственного университета*. 2012. № 4 (108). URL: http://cyberlen inka.ru/article/n/informatsionnaya-bezopasnost-kak-element-informatsionnoy-kultury

8. Прудникова О.В. Феномен інформаційної культури: онтологічний статус та соціоантропологічні детермінанти: монографія / за заг. ред. О.П. Дзьобаня. Харків: Право, 2017. 496 с.

9. Прудникова О.В. Інформаційна культура в інформаційному суспільстві. *Науковий часопис Національного педагогічного університету імені М.П. Драгоманова*: зб. наукових праць; за заг. ред. В.П. Андрущенка. Київ, 2013. Вип. 30 (43). С. 159-166.

10. Дзьобань О. П., Прудникова О. В. Інформаційна та національна культури українського соціуму: проблеми кореляції. *Інформація і право*. № 3(30)/2019. С. 16-27.

11. Бєляков К.І., Онупрієнко С.Г., Шопіна І.М. Інформаційна культура в Україні: правовий вимір: монографія. Київ: КВІЦ, 2018. 169 с.

12. Панченко О.А., Панченко Л.В. Інформаційна безпека та інформаційна культура в сучасному інформаційному суспільстві. *Правова інформатика*. № 2(46)/2015. С. 32-38.

13. Венгеров А.Б. Теория государства и права: учебник для юридических вузов. 3-е изд. Москва: Юриспруденция. 2000. С. 307.

14. Головистикова А.Н., Грудцына Л.Ю. Права человека: учебник. Москва: Эксмо, 2008. С. 125.

15. Шебаніц Д.М. Сучасна проблематика теорії "поколінь прав людини" в умовах європейської міждержавної інтеграції. *Науковий вісник Ужгородського національного університету.* Ужгород: Видавничий дім "Гельветика", 2015. Т. 1. Вип. 31. С. 57-61.

16. Маляренко Т. Безпека людини у мінливому світі: монографія. Донецьк: ТОВ "Східний видавничий дім". 2013. 200 с.

17. Про внесення доповнень до Цивільного Кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету: проект Закону України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=50669

18. Резолюція Парламентської асамблеї Ради Європи 1877 (2012). URL: http://w1.c1.rada.gov. ua/pls/mpz2/docs/1466_rez_1877.htm

19. 0 La Rue F. (26 квітня 2011), Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Doc. A/HRC/17/27, § 85.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 34:004+347.783

ДУБНЯК М.В., *кандидат юридичних наук,* старший викладач кафедри
інформаційного права та права інтелектуальної власності
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського"

ПРОБЛЕМИ ВИЗНАЧЕННЯ ПРАВОВОГО РЕЖИМУ ОБ'ЄКТІВ, СТВОРЕНИХ ЗА ДОПОМОГОЮ ТЕХНОЛОГІЙ НЕЙРОМЕРЕЖ

Анотація. *В статті розглядається механізм створення об'єктів авторського права за допомогою технології штучного інтелекту (на прикладі графічних та музичних творів). З урахуванням особливостей створення таких об'єктів, у статті наведена порівняльно-правова характеристика доцільності поширення на такі об'єкти режиму: авторсько-правової охорони, режиму суспільного надбання, режиму об'єктів, які не мають авторсько-правової охорони, або віднесення до інформаційного об'єкту з режимом з відкритого доступу.*

Ключові слова: *штучний інтелект, нейромережа, інформаційний об'єкт, правовий режим, авторське право.*

Summary. *The article deals with the mechanism of creating copyright objects (e.g. artwork, musical composition) using neural nerworks. Taking into account the peculiarities of the creation of such objects, the article gives a comparative legal description of the expediency of extending to the following legal regimes: objects of copyright, public domain, regime of objects which have no copyright protection or attribution to information object with open access mode.*

Keywords: *artificial intelligence, neural network, information object, legal regime, copyright.*

Аннотация*. В статье рассматривается механизм создания объектов авторского права с помощью технологии искусственного интеллекта (на примере графических и музыкальных произведений). С учетом особенностей создания таких объектов, в статье приведена сравнительно-правовая характеристика целесообразности распространения на такие объекты режима: авторско-правовой охраны, режима общественного достояния, режима объектов, не имеющих авторско-правовой охраны, или отнесения к объектав информационного права с режимом из открытого доступа.*

Ключевые слова: *искусственный интеллект нейросеть, информационный объект, правовой режим, авторское право.*

Постановка проблеми. Поява нових технологій потребує удосконалення правового регулювання суспільних відносин, які неминуче трансформуються через їх використання. Новим викликом системі авторського права є розгляд питання про правовий режим об'єктів, створених за допомогою технологій нейромереж. Актуальність обраної теми пояснюється появою об'єктів, створених за допомогою нейронних мереж, наприклад: Jakedeck, Music Transformer, які створюють музику, проекти: The Next Rembrandt, Deep Dream, додатками Prisma, FaceApp, ZAO, які створюють графічні твори.

Jakedeck – це штучний інтелект для створення музики: будь-який користувач може обрати жанр, темп, інструменти та тривалість треку, назву та отримати свою власну композицію [1]. Music Transformer – заснована на самоаналізі нейронна мережа, яка створює експресивні твори безпосередньо, без використання попередньої шаблонної партитури. Використовуючи таку інноваційну технологію генерування музики, Music Transformer може "писати музику" поза межами навчальних зразків, які вводяться як вихідні дані [2].

The Next Rembrandt – портрет, створений штучним інтелектом на основі аналізу техніки виконання 346 картин митця [3]. Deep Dream – це програмне забезпечення, яке використовує технологію згорткової нейронної мережі для розпізнавання і трансформації візуальних образів [4]. Додаток Prisma за допомогою нейромережі перетворює завантажену фотографію на зображення, схоже за стилем виконання на стиль відомих художників [5].

У 2017 році набуло вірусного поширення програмне забезпечення FaceApp, яке використовує нейромережеві алгоритми для перетворення фотографій або відео в об'єкти образотворчого мистецтва. Ця програма дозволяє виконувати зміну фону або переднього плану, накладання об'єктів один на одного, клонувати/копіювати стиль або ефект з іншого зображення або відео та навіть робити імітацію стилів різних відомих художників. Програма дозволяє робити фотографії або відео шляхом безпосереднього використання додатка, чи завантажувати в додаток вже існуючі фотографії/відео [6].

У вересні 2019 року з'явилось програмне забезпечення ZAO, яке дозволяє замінювати обличчя акторів у фрагментах відеофільму на обличчя користувача [7]. У бібліотеці містяться короткі фрагменти відомих відеофільмів (наприклад, кінофільм "Титанік" з Леонардо Ді Капріо, або фрагменти серіалу "Гра престолів").

Поява таких програмних додатків, що використовують різні нейромережі, та об'єктів, що створені за їх допомогою, визначають мету цього дослідження і обумовлюють необхідність вирішення таких завдань:

1. визначення правового режиму об'єктів, створених за допомогою нейромереж – це інформаційний продукт чи об'єкт авторського права;

2. визначення автора твору, створеного за допомогою технологій штучного інтелекту;

3. визначення режиму такого твору (власне твір, який відповідає усім критеріям охороноздатності, об'єкт, що відноситься до суспільного надбання, об'єкт, що не має авторсько-правової охорони).

Результати аналізу наукових публікацій. Правові проблеми використання технологій штучного інтелекту розглянуто в роботах О.А. Баранова, О.Е. Радутного, Є.О. Харитонова, О.І. Харитонової та інших. Питаннями правового режиму об'єктів авторського права та співвідношення інститутів авторського права та права інтелектуальної власності присвячені роботи таких вчених: А.О. Кодинця, С.В. Мазуренко, С.Й. Литвин, О.П. Орлюк, О.О. Штефан А.С. Штефан та інші. У роботах зазначених науковців проаналізовано технічні особливості функціонування штучного інтелекту та нейромережі, є характеристика видів штучного інтелекту за співставленням можливостей відтворення когнітивних функцій людини. У деяких публікаціях визначено критерії охороноздатності для фотографічних та музичних творів; проаналізовано проблеми розпорядження об'єктами авторського права в частині віднесення таких об'єктів до режиму суспільного надбання за волею автора. Питання про визначення правового режиму об'єктів, створених за допомогою штучного інтелекту, не досліджувалось вітчизняними вченими, що свідчить про актуальність обраного напрямку досліджень.

Виклад основного матеріалу. Нейромережі є одним із видів машинного навчання, а не окремим інструментом.

Нейронна мережа за допомогою штучних нейронів моделює роботу людського мозку, що вирішує певне завдання, самонавчається з урахуванням попереднього досвіду. І з кожним разом робить дедалі менше помилок. Вона застосовується там, де потрібні розпізнавання або генерація зображень і відео, чи використовуються складні алгоритми управління та прийняття рішень, машинний переклад і подібні складні завдання [8].

У вищезазначених проектах використано декілька технологій нейронних мереж. Так, для генерування зображень використовується генеративно-змагальна нейромережа (generative adversarial network – далі GAN). Це алгоритм, який застосовує комбінацію роботи двох нейромереж. Перша генерує (створює) образ, друга намагається відокремити справжні образи від згенерованих. Якщо перший алгоритм запропонував неякісну підробку, яку одразу визначив другий алгоритм, перший алгоритм удосконалює свою роботу, і далі пропонує більш реалістичний образ. За результатами такої сумісної змагальної роботи двох нейромереж можна отримати непоганий результат, адже друга нейромережа визначає очевидні фейки, запропоновані першою.

Для створення музичних творів використовують нейромережу з механізмом моделювання уваги (attention-based neural network). Така технологія визначає наскільки далеко один від одного знаходяться два фрагменти. При цьому мережа "приділяє увагу" повторюваним музичним подіям і може генерувати довгі музичні послідовності. Такий підхід дозволяє моделі узагальнювати навчальні приклади, завдяки чому створювати композиції довшої тривалості [9].

Нейронні мережі використовуються в різних сферах науки та техніки, у тому числі несвідомо застосовуються пересічними громадянами. Багато хто не замислюється, що сучасний смартфон обладнаний такою технологією, яка здатна покращити розпізнавальні якості фотографії, такі як: колір, контрастність, яскравість, експозицію та деякі інші параметри. Під час фотографування алгоритм нейромережі може розпізнавати об'єкти (людей, тварин, пейзажі та інші) та пропонувати інші варіанти композиції, та автоматично здійснювати налаштування світлопередачі під час фотографування [10].

Варто зазначити, що не кожна фотографія охороняється авторським правом, а лише та, що є фотографічним твором. Згідно з міжнародними документами та судовою практикою, існує декілька ознак, які дозволяють виділити критерії охороноздатності фотографічного твору: 1) продукт індивідуальної творчості автора, який виражає його самобутність; 2) становить інтелектуальний витвір автора.

Інколи суди, оцінюючи дотримання критеріїв оригінальності твору, мотивують свої рішення характеристикою процесу створення твору, наприклад: оригінальність прийомів фотографування, прийоми щодо постановки фото, застосування технічних засобів, але утримуються від оцінки результату такого процесу – тобто, самого створеного твору [11].

Не дивлячись на те, що дискусія стосовно визнання фотографій творчими і оригінальними сама по собі триває, у цій публікації ми розглянемо проблему створення фотографій та художніх творів у цифровій формі (далі – об'єкти), за допомогою технологій нейронних мереж.

Для надання об'єкту режиму авторсько-правової охорони, цей об'єкт має відповідати критеріям охороноздатності, такі об'єкти повинні бути створені інтелектуальною, творчою діяльністю людини, мати об'єктивну форму, не залежати від жанру, обсягу і мети призначення, моменту набуття авторського права (не бути пов'язаним із виконанням будь-яких формальностей) [12].

1. Чи можна назвати творчим процес створення об'єктів за допомогою технологій нейронних мереж?

При створенні об'єктів за допомогою технологій нейромережі на сьогодні маємо два способи їх використання. Перший, коли нейромережа видає шаблон твору, а людина вже доповнює його. При цьому важко встановити, було таке доповнення творчим, чи виконано виключно із застосуванням знань та інструментів, запропонованих конкретним програмним продуктом для здійснення графічного редагування.

Як відомо, авторські права не виникнуть у особи, яка здійснює графічне редагування зображень, оскільки ця особа вчиняє механічні, а не творчі дії.

Другий спосіб – користувач завантажує вихідні дані для аналізу (наприклад фотографію), і отримає кінцевий, покращений результат.

Ступінь творчості при створенні об'єктів образотворчого мистецтва можна оцінювати за допомогою неповторності і оригінальності виконання художніх технік конкретним митцем, що надає твору оригінальності, і навіть, "авторського стилю".

У випадку із "творчістю нейромереж" "художня техніка" представлена у вигляді алгоритму, який буде однаково застосовуватись до різних об'єктів. Отже, незалежно від параметрів, які необхідно згенерувати для створення об'єкту, всі вони будуть однакової якості.

Таким чином, головною відмінністю творчості людини від "творчості нейромережі", є вольовий компонент. Нейромережа не ініціює процес створення твору, а виступає засобом для його генерації.

2. Чи мають об'єкти, створені за допомогою нейромереж, автора?

Процес створення об'єкту нейромережею має багаторівневу природу, яка проявляється у наступному.

По-перше, для того, щоб нейромережа створювала шаблони об'єктів, вона повинна бути натренована щодо їх виділення і компіляції. А це, в свою чергу, є інтелектуальна праця програмістів, які програмували алгоритм роботи нейромережі. І відповідно, мають авторські права на частину програмного забезпечення, за допомогою якого працює ця нейромережа.

По-друге, нейромережа навчається на базі конкретних об'єктів, які також можуть охоронятись авторським правом. Теоретично, виникає питання необхідності виплати винагороди авторам, за використання об'єктів їх творчості під час навчання нейромережі.

Разом з тим, з практичної точки зору, практично неможливо визначити, чи відбулося використання конкретного авторського твору під час генерації нового об'єкту нейромережею. Тобто, існує проблема визначення конкретного автора і виплати йому винагороди за використання саме його твору нейромережею.

Дотичним до особливостей генерації об'єктів нейромережею є той факт, що на новий об'єкт не поширюється режим похідного твору.

Відповідно до Закону України "Про авторське право і суміжні права" (далі – Закон) [16] похідним твором є твір, що є творчою переробкою іншого існуючого твору без завдавання шкоди його охороні (анотація, адаптація, аранжування, обробка фольклору, інша переробка твору) чи його творчим перекладом на іншу мову (до похідних творів не належать аудіовізуальні твори, одержані шляхом дублювання, озвучення, субтитрування українською чи іншими мовами інших аудіовізуальних творів).

Ознаками похідного твору є результат творчої переробки іншого твору. Переробка первинного твору не завдає шкоди його охороні. Похідний твір не поглинає фактичну копію первинного твору, а лише використовує її при переробці [13, с. 26-27].

У випадку генерування твору нейромережею проблематично визначити оригінальний твір, з використанням якого відбувається модифікація.

По-третє, до процесу тренування нейромережі залучено велику кількість осіб, які, наприклад, на картинках виділяють певні образи, не замислюючись при цьому, яку саме нейромережу вони тренують.

Отже, всі ці особи забезпечують технічну можливість для становлення нейромережі шляхом її навчання, для майбутнього генерування різних об'єктів.

У суперечках про визнання оригінальності зображення фотографічного твору, сторона може посилатись на підготовку до творчого процесу – перераховувати ті дії, які вона вчинила під час створення твору. Суд, таким чином, може застосувати концепцію "Sweat of the brow" (дослівно "у поті чола"), тобто визнання авторського права на неоригінальний твір завдяки кропіткій роботі автора під час його створення [цит. за 11].

Американська судова практика має цікавий прецедент про встановлення автора серії зображень, зроблених мавпою Наруто, з використанням обладнання, яке належало британському фотографу Девіду Слейтеру [14].

Суперечки виникли через розміщення цих зображень на Вікісховищі, оскільки припускалось, що вони є суспільним надбанням. Вважалось, що дані фотографії не можуть бути суб'єктами авторського права з двох причин. По-перше, зроблені не людиною, а по-друге, фотограф також не може бути їх автором, оскільки він безпосередньо не брав участі у створенні зображень. Фотограф намагався довести, що все обладнання, яким було зроблено фото, належало йому, він самостійно підібрав налаштування, розташував у встановленому місці фотоапарат. Він створив умови для того, щоб це фото могло з'явитися. Спір завершився визнанням фотографа автором зображень.

Для фотографічних творів елементами доказування концепції "Sweat of the brow" можуть бути такі критерії, що свідчать про роботу фотографа, який підбирає технічні характеристики для фотографії, та використовує певні прийоми фотографування. Наприклад, такими критеріями можуть бути: незвичайна композиція, нестандартний ракурс, передача індивідуальності людини в характерній лише для неї манері, особливості комбінації світлотіней, тип освітлення, підібраний автором (денне, штучне, бокове, крапкове, розсіяне), ракурс, діафрагма, фокусна відстань до об'єкта тощо [15, с. 15-16].

Наразі декілька із перелічених функцій містяться у програмних додатках, реалізованих на базі нейромережевої технології, які пропонують користувачу безпосередньо перед фотографуванням, різні варіанти. Або, забезпечують можливість накладення різних світлових фільтрів та об'єктів доповненої реальності, що виключають такі прояви творчості, як підбір композиції, світлотіней, оригінальності під час створення фотографічного твору.

Відзначимо, що важливість прецеденту Naruto v. Slater не стільки у визнанні авторських прав за особою, яка створила технічні умови для створення твору, скільки в самому визнанні об'єктом авторського права твір, який було створено не людиною.

Тобто, програміст, який налаштовує нейромережу і підбирає алгоритми для її поведінки в певних ситуаціях, також створює умови для виникнення твору – однак, сам програміст безпосередньо цей твір не створює. Але як бути з правами інших осіб, які забезпечили доступ до даних, на підставі яких навчалась ця нейромережа? Або як бути з правами інших програмістів, які писали алгоритми? Усі ці особи будуть визнані співавторами? Як визначити відсоток авторського внеску, якщо невідомо, яку частину алгоритму було задіяно нейромережею для створення певного твору? Відповідно до Закону [16], співавторами є особи, спільною творчою працею яких створено твір. Однак ті особи, які забезпечили доступ до даних, на яких навчалась нейромережа, не вчиняють творчих дій. Вони, як і фотограф, забезпечують технічні умови для створення твору.

Враховуючи вищенаведене рішення суду, можна ставити під деякий сумнів необхідність існування критерію "творчості" для визнання об'єкту, створеного за допомогою нейромережі, твором, як необхідної умови поширення режиму авторсько-правової охорони. Тому що вже існує випадок, коли у якості об'єкта авторського права

було визнано твір, створений не людиною, а за допомогою людини, яка лише надала технічні умови для створення об'єкту інтелектуальної власності, однак, безпосередньої участі у процесі "творчої" діяльності не брала.

Окрім проблеми визначення автора, існує проблема щодо визначення строку правової охорони.

Відповідно до Закону [16] авторське право діє протягом усього життя автора, і 70 років після його смерті. А для нейромережі цей строк прирівнюється до ...вічності? Як можна оцінити життя нейромережі?

Формулювання у Законі [16] "життя автора" може застосовуватись для правового регулювання в системі "людина-людина", однак не актуальна в системі "людина-машина" та "машина-машина".

3. Правовий режим суспільного надбання.

Суспільне надбання – це такі твори літератури, науки та мистецтва, щодо яких не виникла чи припинилась правова охорона, і відповідно відсутня виключність у їх використанні.

Поняття "суспільне надбання" можна розділити на два значення – широке та вузьке. Так, у широкому розумінні, суспільне надбання – це можливість для вільного використання будь-якою особою об'єкту авторського права. У вузькому розумінні суспільне надбання – це наявність деяких об'єктів авторського права, які ніколи не мали правової охорони, і (або) правова охорона на які перестала діяти у зв'язку з закінченням строку її дії [17, с. 214].

Відповідно до ст. 30 Закону [16] закінчення строку дії авторського права на твори означає їх перехід у суспільне надбання. Таким чином, режим суспільного надбання можна поширити лише на твори, які охоронялись авторським правом, а не шляхом визначення переліку об'єктів, які можуть вільно використовуватись у зв'язку із тим, що не є творами.

ЦК України в Гл. 75 визначив два основних способи розпорядження об'єктами права інтелектуальної власності: за договором про передання виключних майнових прав інтелектуальної власності, і за договором про надання права використовувати об'єкт права інтелектуальної власності. Питання передачі творів правоволодільцем в суспільне надбання – як способу розпорядження виключним правом – законодавством не врегульовані [18, с. 120].

Згідно із статтею 1108 ЦК України особа, яка має виключне право дозволяти використання об'єкта права інтелектуальної власності (ліцензіар), може надати іншій особі (ліцензіату) письмове повноваження, яке надає їй право на використання цього об'єкта в певній обмеженій сфері (ліцензія на використання об'єкта права інтелектуальної власності).

Ліцензія може бути виключною, одиничною, невиключною, а також іншого виду, що не суперечить закону. Під іншою ліцензією можна розуміти групи ліцензій Creative Commons, однак, передбачається наявність ліцензіата, а не встановлення режиму використання твору для необмеженої кількості осіб. Тому режим ліцензування твору не може розглядатись як правовий механізм відмови автора від майнових прав, чи їх припинення за волею автора.

Відповідно до ст. 1113 ЦК України договір про передачу виключних майнових прав інтелектуальної власності – це договір, за яким одна сторона (особа, що має виключні майнові права), передає другій стороні, частково або у повному складі, ці права відповідно до закону, та на визначених договором умовах. Оскільки, правовий режим суспільного надбання передбачає можливість кожного вільно використовувати

твір, то договір про передання виключних майнових прав не може бути договором про передачу цих прав всьому суспільству, адже законом передбачено наявність саме другої сторони, до якої переходять усі права та обов'язки стосовно об'єкта права інтелектуальної власності.

Таким чином, для того, щоб поширити режим суспільного надбання на твори створені за допомогою нейромережі, необхідно вирішити первісне протиріччя. Суть такого протиріччя полягає у тому, що такі об'єкти мають спочатку бути визнані об'єктами авторського права із встановленням строку їх правової охорони, припинення якого обумовить перехід в режим суспільного надбання.

4. Правовий режим об'єктів, що не охороняються авторським правом.

Відповідно до статті 10 Закону [16], статті 434 ЦК України, об'єктами, що не охороняються авторським правом, є: 1) повідомлення про новини дня або поточні події, що мають характер звичайної прес-інформації; 2) твори народної творчості (фольклор); 3) офіційні документи політичного, законодавчого, адміністративного характеру та їх офіційні переклади; 4) державні символи України; 5) грошові знаки; 6) бази даних, що не відповідають критеріям оригінальності і на які поширюється право sui-generis.

Частина цих об'єктів має інформаційний характер, необхідна суспільству для його функціонування (наприклад, повідомлення про новини дня, офіційні документи, державні символи України, грошові знаки). Щодо інших: неможливо встановити авторство, коли об'єкти створені колективним творчим внеском усього народу (фольклор). Решта об'єктів – не відповідає критеріям творчості та оригінальності, і є технічним упорядкуванням інформації. Критерії такого упорядкування і представлення інформації не є творчими, наприклад: за алфавітом, за числовим покажчиком, за часом настання (телефонні довідники, розклади телерадіопередач, розклади руху транспортних засобів,)

Отже, створення об'єктів за допомогою нейромережі, очевидно, є також об'єктом, який не повинен мати режиму авторсько-правової охорони, через відсутність творчого характеру і технічного способу представлення інформації у вигляді, що видається алгоритмом нейромережі як графічний об'єкт з покращеними якостями. Наприклад, правильної кольорової гами, світлопередачі, яскравості-контрасту, оскільки в базі нейромережі міститься численна інформація про приклади використання аналогічних зображень.

5. Правовий режим інформації.

Відповідно до ст. 1 Закону України "Про інформацію", інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях, або відображені в електронному вигляді. При цьому дані – це багатозначне поняття, в якому можуть бути дані як форма представлення знань, у буквенно-цифровому, числовому, текстовому, звуковому, або графічній формі [19].

Можемо припустити, що об'єкт, створений за допомогою нейромережі, має ознаки об'єкта саме інформаційного права, у формі інформації, та повинен мати режим інформації з відкритим доступом.

Технічно розрізнити об'єкт авторського права та об'єкт, створений за допомогою ШІ, можна через метадані про файл, які містять назву програми, в якій було створено такий об'єкт, або за допомогою спеціального програмного забезпечення. Без використання спеціальних програм відрізнити об'єкт, створений за допомогою нейромережі, або людиною, яка працювала у графічних редакторах, неможливо.

Погодимось із думкою А. Кодинця, який вважає, що в умовах інформаційного суспільства, розвитку наукової та науково-технічної діяльності, монопольне право

суб'єкта інтелектуальної власності потребує істотних обмежень як у часовому, так і у просторовому вимірах. Важливою тенденцією розвитку правового регулювання інтелектуальної діяльності в інформаційному суспільстві є поступове послаблення системи охорони інтелектуальної власності, впровадження нормативних змін, спрямованих на забезпечення збалансованого поєднання інтересів творців і їх правонаступників в отриманні винагороди, та членів суспільства у праві на доступ до інформації, її поширення і використання [20, с. 19].

Висновки.

Враховуючи повсюдне впровадження технологій нейромереж, кожен користувач має володіти інформацією про те, які саме функції програмного забезпечення використовують цю технологію, аби уникнути ситуації створення об'єкту без творчого внеску. Та мати можливість відключення подібних функцій без блокування доступу до використання технології.

Багаторівнева природа створення об'єктів за допомогою технологій нейромереж, не робить їх самодостатніми, адже з теоретичного боку може породжувати такі режими як: співавторство, похідний твір, що значно ускладнює визначення авторського внеску під час створення об'єкта. А з практичної точки зору, довести факт співавторства чи наявності ознак оригінального твору у згенерованому об'єкті проблематично.

Правовий режим суспільного надбання не може застосовуватись до об'єктів, створених за допомогою нейромереж. Оскільки такі об'єкти спочатку мають бути віднесені до об'єктів авторського права, із встановленням строку їх правової охорони, припинення якого обумовить перехід в режим суспільного надбання.

Враховуючи технічні характеристики та особливості створення об'єктів з використанням технології нейромереж, правовий режим інформації з відкритим доступом, та віднесення до неохоронюваних об'єктів авторського права, є найбільш обґрунтованим для правового регулювання об'єктів, створених за допомогою технології нейромереж.

Використана література

1. Dredge S. Jukedeck hopes artificial intelligence can 'democratise music'. URL: https://musically.com/2017/08/09/jukedeck-artificial-intelligence-music (дата звернення 07.12.2019).

2. Google Music Transformer: композитор на базі штучного інтелекту. URL: http://innotech news.com/corporations-news/2388-google-music-transformer-kompozitor-na-baze-iskusstvennogo-intellekta (дата звернення 07.12.2019).

3. The Next Rembrandt. URL: https://news.microsoft.com/europe/features/next-rembrandt (дата звернення 07.12.2019).

4. DeepDream. URL: https://en.wikipedia.org/wiki/DeepDream (дата звернення 07.12.2019).

5. Prisma Terms of Use URL: https://prisma-ai.com/terms.html (дата звернення 10.09.2019).

6. FaceApp: Terms of Use 08.03.2017. URL: https://www.faceapp.com/terms (дата звернення 10.09.2019).

7. ZAO: Terms of Use 07.09.2019. URL: https://h5.ai-factory.com/zao/static-pages/protocol.html ?name=privacy (дата звернення 10.09.2019).

8. Штучний інтелект, машинне навчання та нейронні мережі – у чому різниця і для чого їх використовують. URL: https://evergreens.com.ua/ua/articles/machine-learning-overview.html (дата звернення 10.09.2019).

9. Google Brain представили сеть Music Transformer для создания гармоничной музыки URL: https://neurohive.io/ru/novosti/music-transformer (дата звернення 10.09.2019).

10. Ivan Mityazov ШІ в смартфонах – використанян і подальші перспективи. URL: https://root-nation.com/articles-ua/tech-ua/ua-ai-smartphones (дата звереннння 09.09.2019).

11. Томаров І. Оригінальність фотографії у судовій практиці. URL: http://www.legalshift.com.ua/?p=948 (дата звереннння 09.09.2019).

12. Штефан О. Поняття об'єкту авторського права та критеріїв його охороноздатності. *Теорія і практика інтелектуальної власності*. 2006. № 6. С. 3-8

13. Штефан А.С. Авторське право і суміжні права: особливості правової охорони, здійснення та захисту: монографія – (НДІ інтелектуальної власності НАПрНУ). Київ: ТОВ "НВП Інтерсервіс", 2017. 150 с. (дата звернення 07.12.2019).

14. Naruto v. Slater, No. 16-15469 (9th Cir. 2018) URL: https://law.justia.com/cases/federal/appellate-courts/ca9/16-15469/16-15469-2018-04-23.html (дата звернення 17.08.2019).

15. Мазуренко С.В. Авторське право на фотографії. Актуальні проблеми держави і права. 2008, С. 12-19.

16. Про авторське право і суміжні права: Закон України від від 04.11.18 р. № 3792-XII URL: https://zakon.rada.gov.ua/laws/show/3792-12 (дата звернення 17.08.2019).

17. Право інтелектуальної власності: акад. курс: підруч. для студ. вищих навч. закладів / О.П. Орлюк, Г.О. Андрощук, О.Б. Бутнік-Сіверський та ін.; за ред. О.П. Орлюк, О.Д. Святоцького. Київ: Видавничий Дім "Ін Юре", 2007. 696 с. (дата звернення 10.09.2019).

18. Литвин С.Й. Окремі питання щодо припинення виключних майнових прав на твір *Право*. 2015. № 3. С. 116-122.

19. Дані. URL: https://uk.wikipedia.org/wiki/Дані (дата звернення 09.09.2019).

20. Кодинець А. Інтелектуальна власність та інформаційні відносини: теоретичні засади правового регулювання. *Підприємництво, господарство і право*. 2016. № 8. С. 16-20.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

Правова інформатика

УДК 34:004

БЕЖЕВЕЦЬ А.М., аспірантка Національного технічного університету України
“Київський політехнічний інститут імені Ігоря Сікорського”

ОСОБЛИВОСТІ СУБ’ЄКТНОГО СКЛАДУ ІНФОРМАЦІЙНИХ ВІДНОСИН В УМОВАХ ІНДУСТРІЇ 4.0

Анотація. *Стаття присвячена дослідженню сучасного стану наукових ідей та концепцій інформаційних відносин в умовах четвертої промислової революції. З огляду на потенційно можливу експансію штучного інтелекту розглянуто сучасні теорії суб’єкта права та особливості суб’єктного складу інформаційних відносин.*

Ключові слова: *інформаційні відносини, робот, штучний інтелект, робототехніка, правовий статус робота, правосуб’єктність робота, електронна особа, Індустрія 4.0, четверта промислова революція*

Summary. *The article is devoted to the study of the current state of scientific ideas and concepts of information relations in the conditions of the fourth industrial revolution. Given the potential expansion of artificial intelligence, modern theories of the subject of law and features of the subject composition of information relations are considered.*

Keywords*: robot, artificial intelligence, robotics, the legal status of robot, legal personality of robots, electronic person, Industry 4.0, the fourth industrial revolution.*

Аннотация. *Статья посвящена исследованию современного состояния научных идей и концепций информационных отношений в условиях четвертой промышленной революции. Учитывая потенциально возможную экспансию искусственного интеллекта, рассмотрены современные теории субъекта права и особенности субъектного состава информационных отношений.*

Ключевые слова*: робот, искусственный интеллект, робототехника, правовой статус робота, правосубъектность робота, электронное лицо, индустрия 4.0, четвертая промышленная революция.*

Постановка проблеми. Цілеспрямований розвиток інформаційних відносин, зростання обсягу застосування новітніх інформаційних технологій призвів до формування інформаційного суспільства, яке характеризується, перш за все, переорієнтацією економіки з використанням матеріальних ресурсів на ефективне впровадження знання технологій. Стрімкий розвиток інформаційно-комунікаційних технологій, який спостерігається останнім часом, спрямований на суцільну роботизацію та автоматизацію виробництва. Крім того, враховуючи існуючі тенденції, цифровізація торкнеться і повсякденного життя кожної людини. Вже зараз важко уявити сучасну людину без гаджетів в кишенях, комп’ютера та іншої техніки вдома, в офісі. На вулицях почали з’являтися безпілотні автомобілі та автобуси, господарю квартири допомагає система “розумний дім”, за допомогою смарт-контрактів можна заощадити час та гроші.

Наразі світ стоїть на порозі четвертої промислової революції, результати якої в недалекому майбутньому стануть повсякденними явищами в житті кожної людини та суспільства в цілому. За прогнозами Всесвітнього Економічного Форуму, більшість технологій четвертої промислової революції стане повсякденністю вже в 2027 році [1].

Зміни в суспільних відносинах потребують відповідної модернізації системи їх регулювання, зокрема, за допомогою правових норм. У звязку з цим необхідним є осучаснення існуючої законодавчої бази на підставі ідей та концепцій, які формують правову доктрину.

Результати аналізу наукових публікацій. Питанню структури інформаційних правовідносин та суб'єктного складу, як обов'язкового елементу правовідносин, присвячені наукові дослідження, що знайшли своє відображення у працях І.В. Арістової, О.А. Баранова, Т.А. Костецької, О.В. Синєокого, А.І. Марущака, Г.Г. Чмерук, М.В. Фігель. Окреслена проблема неодноразово ставала об'єктом наукового інтересу багатьох інших науковців через важливість та невідкладність її розгляду для науки та практики. Аналізуючи праці названих науковців, автор вважає актуальним науковим завданням дослідження трансформації уявлення про суб'єктний склад інформаційних відносин на сучасному етапі науково-технічного прогресу.

Метою статті є визначення сучасного стану правового регулювання інформаційних відносин, особливостей їх суб'єктного складу та перспектив подальшого удосконалення законодавства у цій сфері.

Виклад основних положень. Науково-технічний прогрес завжди спрямований та неодмінно призводить до підвищення ефективності виробництва, зменшення витрат та часу на виробничі процеси, збільшення прибутків власників. Нові креативні та інноваційні моделі обслуговування створюють революцію в сфері послуг і виробництва. Як свідчить історія, цей процес відбувається не еволюційним, а революційним шляхом, представляючи доволі нетривалий проміжок часу порівняно із періодом існування людства.

Майже 250 років тому відбулася так звана перша індустріальна революція, яка стала початком індустріальної ери та отримала назву Індустрія 1.0. Саме в цей період людина почала активно запроваджувати машинну автоматизацію. І хоча це були лише найпростіші механічні пристрої, розпочався масштабний процес механізації, коли речі (товари) створювалися не людською працею, а машинами. Поява парового двигуна, розвиток важкої промисловості, використання вугілля в якості основної енергії стали рушійною силою потужної індустріалізації людства.

Друга промислова революція пов'язана з електрифікацією виробництва, що допомогло автоматизувати виробничі процеси, а як наслідок – прискорити темпи та масштаби виробництва.

Особливістю третьої промислової революції стала подальша автоматизація та комп'ютеризація, при чому не лише виробничої сфери, а й побуту людей. Цей етап припадає на 1960 – 1970 роки та характеризується впровадженням електроніки та інформаційних технологій в серійне виробництво із відповідною мінімізацією участі людини у такому процесі.

Відзначаючи значний розвиток механізації та автоматизації виробництва у визначений двохсотрічний період, все ж є підстави зазначити, що все одно всі виробничі процеси потребують участі людини.

Принциповою відмінністю четвертої промислової революції, або Індустрії 4.0 є застосування новітніх технологій, які поєднають фізичне, біологічне та цифрове середовище. При чому це стосуватиметься не лише економіки, сфери виробництва, а й практично всіх сфер життя людини. З їх допомогою стає можливим створення "самоорганізованого" виробництва: люди, машини, заводи, логістика та продукти взаємодіють, в тому числі безпосередньо один з одним. Така абсолютно нова модель

побудови промислових зв'язків може бути реалізована виключно шляхом цифрової модернізації існуючих відносин.

Цифровий (пов'язаний з Інтернетом) підхід зачіпає всі етапи життєвого циклу продукту, включаючи дизайн і створення прототипу, наладку і обслуговування виробничої лінії, контроль і оптимізацію виробництва, а також дані, отримані в результаті зворотного зв'язку від клієнтів і споживачів.

Однією з базових технологій, за допомогою яких стануть можливі такі зміни у виробництві, називають Інтернет речей (далі – IoT), який являє собою сукупність технологій, що забезпечують підключення до Інтернету будь-яких об'єктів для їх автономної роботи без участі людини. Різновидом IoT визначають промисловий (індустріальний) Інтернет речей, що стане основою автоматизації виробництва і побуту в майбутньому, хоча його вплив відчутний вже зараз. Існування IoT є невід'ємним елементом Індустрії 4.0.

Термін "Індустрія 4.0", скорочено – I 4.0 або просто I 4 був публічно представлений в 2011 році на Ганноверському ярмарку [2] та отримав свою назву від ініціативи (програми), очолюваної бізнесменами, політиками і вченими, які визначили її як засіб підвищення конкурентоспроможності промисловості Німеччини. Її суть полягає в інтеграції у виробничі процеси так званих кіберфізичних систем (CPS), які працюють за допомогою Інтернета і здатні самостійно (автономно, без втручання людини) контролювати, прогнозувати та за необхідності змінювати традиційні шаблони дій з метою оптимізації виробництва. Індустрія 4.0 докорінно змінює не тільки процес виробництва, але і сферу послуг, пов'язаних з продукцією, що випускається.

Індустрія 4.0 являє собою початок складного трансформаційного процесу, який глибоко вплине не лише на промисловість, а й суспільство в цілому шляхом цифровізації бізнесу, економіки, суспільних відносин. Таке перетворення засноване на зближенні реального (аналогового) світу і віртуального (цифрового) світу за допомогою машинно-машинного (M2M) зв'язку, автономних систем (наприклад, робототехніки) та IoT. Використання віртуальної реальності, застосування технології блокчейн, створення цифрових платформ для інтеграції IoT з метою моніторингу та управління бізнес-процесами, аналітика великих даних із застосуванням хмарних обчислень і штучного інтелекту стануть невід'ємними ознаками Індустрії 4.0.

Кожен із зазначених вище етапів індустріалізації став поштовхом для нового етапу розвитку суспільства. Невід'ємним елементом кожного з етапів стала наявність машин (механізмів, роботів), що тим чи іншим шляхом впливало на суспільні відносини.

Зрозуміло, що на перших етапах індустріалізації суспільства вплив цих об'єктів є мінімальним та опосередкованим. До особливих змін в суспільних та правових відносинах це не призвело. Проте на сьогоднішній день є достатні передумови для трансформації суспільних відносин, їх правового регулювання, зміни суб'єктно-об'єктного складу.

Трансформація відносин може відбутися лише через трансформацію суспільної свідомості, з розумінням того, що синергія людини і машини неминуча. Саме в сучасний період розвитку суспільства закладено фундамент для подальшого стрімкого розвитку робототехніки, зокрема, залучення роботів зі штучним інтелектом практично у всі сфери життя людини.

Такі процеси потребують цілеспрямованого впливу держави з метою впорядкування та стабілізації нових суспільних відносин шляхом законодавчого закріплення змін та регулювання відносин за допомогою правових норм.

Різновидом відносин, які неодмінно зазнають змін, є інформаційні правовідносини. На даний час відсутнє єдине доктринальне визначення інформаційних відносин, при цьому багато науковців формулюють визначення таких відносин, акцентуючи увагу на їх певних ознаках, без урахування всієї сукупності та специфіки.

Із наявних в науковому просторі дефініцій, на думку автора, підставно виділити наступні. Як зазначає М.В. Фігель, інформаційні правовідносини – це урегульовані нормами інформаційного права суспільні відносини, учасники яких виступають носіями юридичних прав і обов'язків, що регулюють приписи щодо створення, розподілу та використання інформації, які містяться в цих нормах [3, с. 234].

На думку О.В. Синєокого, інформаційні правовідносини – це суспільні відносини, які виникають під час створення, розподілу та використання інформації та врегульовані нормами інформаційного права, учасники якого володіють відповідними юридичними правами та обов'язками [4, с. 98].

В.М. Боер, О.Г. Павельєва вважають [5, с. 51], що інформаційні правовідносини необхідно поділити на безпосередньо інформаційні правовідносини та відносно-визначені інформаційні правовідносини. Під безпосередньо інформаційними правовідносинами треба розуміти відносини, що виникають з приводу створення інформації, визначення прав власності на неї (з наданням права володіння, користування та розпорядження), а також її обігу (передачі іншим суб'єктам, обробки, аналізу, переробки, споживання) та захисту.

Проаналізувавши наведені вище дефініції, вважаємо за доцільне узагальнити висловлені думки та визначити інформаційні відносини як суспільні відносини щодо створення, фіксації, поширення, пошуку, отримання, зберігання інформації, які регулюються нормами законодавства, виникають, розвиваються та припиняють свою дію в інформаційному просторі між суб'єктами права, які наділені інформаційними правами та обов'язками.

Таким чином, обов'язковому правовому регулюванню підлягають такі суспільні відносини, які здійснюються в інформаційному просторі відносно специфічного об'єкта – інформації та формуються між специфічними суб'єктами.

Чинне законодавство під інформацією розуміє будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді (ст. 1 Закону України "Про інформацію", ст. 200 Цивільного кодексу України). Автором не заперечується специфічний характер інформації, пов'язаний із множинністю її джерел, носіїв, способів відображення тощо. І хоча феномен інформації представляє постійний науковий інтерес і потребує подальшого дослідження, однак це не є предметом цієї роботи, а сприймається як факт (твердження). Натомість вважаємо актуальним науковим завданням дослідження трансформації уявлення про суб'єктний склад інформаційних відносин на сучасному етапі науково-технічного прогресу.

Тривалий час єдиним суб'єктом відносин, пов'язаних із створенням та поширенням будь-якої інформації, була людина, оскільки лише вона мала інтелектуальні переваги. Свої знання, досвід передавалися людьми із покоління в покоління, спочатку усно, а з появою писемності – за допомогою літер, нанесених на спеціально обробленій шкірі тварин, папірусі, дереві, камені тощо.

Пізніше до суб'єктного складу суб'єктів інформаційних відносин почали входити держави, юридичні особи приватного і публічного права. Більш того, у наші часи вже існує думка про те, як писав зокрема А. Марущак, – ми, можливо, на сьогодні перебуваємо напередодні виникнення нових учасників інформаційних відносин, якими зможуть стати новітні інформаційні технології, наділені штучним інтелектом [6]. Це

питання на сьогодні стає дедалі більш актуальним і не лише для України, а й на міжнародному рівні.

І хоча роботи зі штучним інтелектом ще не стали звичайним явищем в суспільстві, а деякі науковці висловлюють обґрунтований сумнів щодо реалізації такого сценарію в найближчому майбутньому, це не означає, що такий виклик можна ігнорувати.

Цифрові дані оточують людину протягом вже тривалого часу, постійно зростаючи в кількості та якості. Інтернет речей, 3D-друк, застосування роботів зі штучним інтелектом в різноманітних процесах людської діяльності та інші яскраві новинки в сфері автоматизації вже стали невід'ємними атрибутами сучасного інформаційного суспільства.

Величезний масив цифрових даних являє собою середовище, в якому є можливість висвітлювати різні події реального світу, які не знаходять свого відображення в іншому (аніж цифровому) вигляді. Людина здатна на розпізнавання цих подій, однак лише при зручному відображенні і на доступних для сприйняття масштабах інформації. Наприклад, людина здатна ідентифікувати наявність предмета на фотографії, але не впорається, якщо перед нею будуть мільйони фотографій. Для роботи з таким масштабом даних стає доцільним машинними (автоматизованими) методами обробити і структурувати масив цифрових даних, визначивши та виокремивши необхідні.

Добре відомими прикладами з галузі робототехніки і штучного інтелекту є так звані "розумні" фабрики, автомобілі без водія, безпілотники доставки. Уже зараз роботи можуть бути використані в різних сферах життя суспільства, наприклад, замість солдатів, для військової промисловості, в медицині для проведення надскладних і точних операцій, в соціальній сфері роботи можуть подбати про літніх людей тощо.

Останнім часом досягнуто значних успіхів у сфері створення роботів зі штучним інтелектом, нанороботів, габаритні розміри яких дорівнюють молекулі, впроваджується вживлення в організм людини мікрочипів, клонування тканин, кліток, органів, друк органів на 3D-принтері. Завдяки цьому можливим прецедентом стане створення кіборга – людини з кібернетичним організмом.

Штучний інтелект (далі – ШІ) – це кіберфізична система, яка працюючи в автономному від людини режимі, здатна до самовдосконалення. Це величезна перевага ШІ для Індустрії 4.0 сьогодні, але при цьому серйозний виклик в майбутньому, адже людина може втратити свою інтелектуальну перевагу, а відтак – панівне становище при прийнятті рішень та визначенні стратегії поведінки.

З метою упередження можливих загроз, актуалізації правового регулювання суспільних відносин з таким елементом, необхідним є формування єдиного нормативного підходу на міжнародному рівні у визначенні правового статусу суб'єктів інформаційних відносин.

П'ять основних ринків промислових роботів становлять 74 відсотки глобальних установок у 2018 році: Китай, Японія, Республіка Корея, США та Німеччина [7]. Зазначеному повсюдному впровадженню роботів передує створення відповідної правової бази.

Зокрема, у 2015 році Урядом Японії було затверджено Нову стратегію роботів (New Robot Strategy), а також створено Національний інститут просування цифрової економіки і цифрового суспільства. В грудні 2017 року в конгрес США був внесений проект закону, який закріплює визначення поняття штучного інтелекту в законодавстві США. У червні 2017 року в Німеччині було затверджено збірку етичних норм для роботизованих транспортних засобів (звіт Комісії з етики Федерального міністерства транспорту і цифрової інфраструктури Німеччини "Автоматизоване та під'єднане керування").

До перших кроків глобального законодавчого врегулювання питання правового статусу роботів та штучного інтелекту можна віднести Резолюцію, що у 2017 році розглянуто Комітетом Європейського Парламенту з правових питань, яка містить пропозицію включити в законодавство ЄС поняття "розумний робот", розробити систему реєстрації таких роботів, а також визначити правовий статус роботів як електронної особистості (електронної особи) [8]. Саме питання визначення правосуб'єктності роботів викликає на сьогодні значний резонанс в науковій та практичній сфері серед науковців та практиків у всьому світі.

Українське законодавство є абсолютно не готовим до таких новел, хоча на теоретичному дослідницькому рівні дискусія з цього приводу набирає значних обертів.

Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки, схвалена Розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р. [9] визначає необхідність створення оновленої концепції "розумного виробництва", що ототожнюється з "четвертою промисловою революцією" та появою кіберфізичних систем. Індустрія 4.0 – наступний етап цифровізації виробництв та промисловості, на якому головну роль відіграють такі технології та концепти, як Інтернет речей, "Великі Дані" (Big Data), "предиктивна аналітика", "Хмарні обчислення", "машинне навчання", машинна взаємодія, штучний інтелект, робототехніка, 3D-друк, доповнена реальність.

Відповідно до статті 4 Закону України "Про інформацію" суб'єктами інформаційних відносин є фізичні особи; юридичні особи; об'єднання громадян; суб'єкти владних повноважень. І хоча традиційно під фізичними особами розуміють громадян, іноземців, осіб без громадянства; під юридичними особами – підприємства, установи, організації всіх форм власності; під суб'єктами владних повноважень – державу, територіальні громади, державні та місцеві органи влади, однак це не дає підстав для розширеного тлумачення цієї норми з можливістю включення до суб'єктного складу інформаційних правовідносин інших суб'єктів.

При дослідженні питання поняття суб'єкта інформаційного права Т.А. Костецька вказує, що суб'єкти інформаційного права – це юридичні й фізичні особи, які наділені правосуб'єктністю і потенційно можуть стати учасниками інформаційних правовідносин [10, с. 69].

О.А. Баранов зазначає, що суб'єкт інформаційного права – це особа, яка володіє правосуб'єктністю, тобто потенційно здатна бути учасником інформаційних правовідносин. А суб'єкт інформаційних правовідносин – це реальний учасник конкретних правовідносин [11, с. 49].

І.В. Арістова вважає, що суб'єкти інформаційних правовідносин – це особи, які беруть участь у конкретних правовідносинах і які є носіями інформаційних обов'язків та прав [12, с. 67].

Таким чином підставно дійти висновку, що обов'язковою ознакою (властивістю) участі в інформаційних відносинах є наявність у особи правосуб'єктності.

Враховуючи, що правосуб'єктність не надається виключно людині, а також те, що саме законодавець визначає суб'єктний склад учасників правовідносин, можна дійти висновку, що законом правосуб'єктність може бути поширена і на інших осіб, тому надання роботу зі штучним інтелектом особливого суб'єктного статусу, зокрема, статусу електронної особи цілком можливе за умови створення відповідної норми. Наділення роботів зі штучним інтелектом правосуб'єктністю не означає набуття ними прав та обов'язків людини та не повинно бути спрямованим на уникнення відповідальності іншими суб'єктами.

Висновки.

Сучасний розвиток робототехніки, Індустрія 4.0, цифровий бізнес, цифрова економіка та подальший рух в напрямку розвитку цифрового суспільства створюють передумови для формування правової бази, здатної забезпечити функціонування оновлених суспільних відносин. Виробництво з підтримкою IoT передбачає збір даних в реальному часі і обмін ними між різними виробничими ресурсами, такими як машини, матеріали і робочі місця. Зв'язок M2M, IoT і автономних машин та пристроїв в рамках I4.0 відкривають дивовижні можливості для бізнесу. Однак, одночасно, ці досягнення створюють нові правові проблеми, які повинні бути вирішені невідкладно.

Сучасний стан законодавчого забезпечення є застарілим і не відповідає новим викликам. Можливості (властивості) штучного інтелекту дають підстави надати йому правосуб'єктності для визнання суб'єктом правовідносин з наділенням його правовим статусом електронної особи. А враховуючи, що така функція належить виключно державі, автор вважає за доцільне прискорити законотворчу діяльність в цьому напрямку.

Використана література

1. Harnessing the Fourth Industrial Revolution for Sustainable Emerging Cities. URL: http://www3.weforum.org/docs/WEF_Harnessing_the_4IR_for_Sustainable_Emerging_Cities.pdf

2. Чмерук Г.Г. Економічні, соціальні та психологічні виклики Індустрії 4.0. *Economics and Finance*. 2018. № 6. С. 61-68. URL: http://dspace.ubs.edu.ua/jspui/bitstream/123456789/1445/1/chmeruk_the_economic_social.pdf

3. Фігель М.В. Доступ до інформації та електронне урядування. Київ: Факт, 2004. 336 с.

4. Синєокий О.В. Високотехнологічне інформаційне право України. Харків: Право, 2010. 360 с.

5. Боер В.М., Павельева О.Г. Информационное право: учеб.пособие. Ч. 1. С-Пб.: ГУАП, 2006. 116 с.

6. Марущак А. Поняття суб'єктів інформаційних правовідносин та їх класифікація *Правова інформатика*. № 4(12)/2006. С. 44-48. URL: http://ippi.org.ua/sites/default/files/06maipk.pdf

7. Industrial Robots: Robot Investment Reaches Record 16.5 billion USD. URL: https://ifr.org /ifr-press-releases/news/robot-investment-reaches-record-16.5-billion-usd

8. European Civil Law Rules In Robotics. URL: https://www.europarl.europa.eu/ RegData/ etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf

9. Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки: Розпорядження КМ України від 17.01.18 р. № 67. URL: https://zakon.rada.gov.ua/go/67-2018-%D1%80

10. Костецька Т.А. Актуальні проблеми державно-правового регулювання інформаційних відносин. *Часопис Київського університету права*. 2006. № 4**.** С. 63-68.

11. Баранов О. Інститути інформаційного права. *Правова інформатика*. № 3(11)/2006. С. 40-46.

12. Арістова І.В. Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. …д-ра юрид. наук: 12.00.07 / І. В. Арістова. Харків, 2002. 476 с.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 681.3:314.1:004.6

БРАЙЧЕВСЬКИЙ С.М., *кандидат фізико-математичних наук*

ПРОБЛЕМА ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ З ЕЛЕМЕНТАМИ ШТУЧНОГО ІНТЕЛЕКТУ

Анотація. *В роботі розглядаються можливі механізми неконтрольованої генерації наборів персональних даних системами Інтернету речей з елементами штучного інтелекту*

Ключеві слова:*інформаційні технології, Інтернет речей, персональні дані.*

Summary. *Possible mechanisms of uncontrolled generation of sets of personal data by systems of the Internet of things with elements of artificial intelligence are considered in the work*

Keywords: *information technology, Internet of Things, personal data.*

Аннотация. *В работе рассматриваются возможные механизмы неконтролируемой генерации наборов персональных данных системами Интернета вещей с элементами искусственного интеллекта*

Ключевые слова: *информационные технологии, Интернет вещей, персональные данные.*

Постановка проблеми. Швидкий розвиток сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують ретельного вивчення. До їх числа відносяться і проблеми правового регулювання, пов'язані з використанням Інтернету речей (далі – ІР) [1 – 6]. Вони пов'язані з наявністю (принаймні, гіпотетичною) в поведінці систем ІР-елементів соціальної поведінки [2]. Питання про природу соціальних відносин між людиною та технологічною системою є, взагалі кажучи, досить нетривіальне. В пропонованій роботі ми не маємо наміру обговорювати цю проблему в повному обсязі.

Однією з проблем, які активно обговорюються у зв'язку з розвитком ІР, є захист персональних даних [7; 8]. Причина полягає перш за все в тому, що системи ІР за своєю природою призначені для збирання різноманітних даних, причому відповідно до певних алгоритмів, які не завжди відповідають загальноприйнятим нормам оперування конфіденційними відомостями. Важливо, що значна частина ризиків, що виникають, взагалі не пов'язані з штатними режимами експлуатації систем ІР. Дійсно, кібернетична система може оперувати даними, "не усвідомлюючи", що вони означають чи можуть означати в суб'єктивному сприйнятті людиною. Машина використовує дані з певною метою, тоді як хтось може використати ці ж самі дані зовсім з іншою метою.

В наявній літературі загалом обговорюються ситуації, пов'язані з безпосереднім отриманням даних за допомогою датчиків ІР та їх можливе несанкціоноване розповсюдження шляхом використання мережних технологій. Але мають бути розглянуті й складніші ситуації, що можуть виникати в процесі експлуатації систем, які містять елементи штучного інтелекту. В таких ситуаціях машина може оперувати даними, які вона самостійно збирає та опрацьовує в процесі вирішення задач, що виходять за межі лінійної обробки інформації, типової для "звичайних" кібернетичних систем.

В пропонованій роботі ми проаналізуємо принципову здатність систем з елементами штучного інтелекту в процесі експлуатації самостійно модифікувати алгоритми, закладені в них проектувальниками. А це означає, що вони можуть неконтрольовано генерувати непередбачені набори даних, які за своєю природою мають

бути віднесені до категорії персональних даних. Результатом може бути створення якісно нових комплексів персональних даних, які відсутні в інших наявних джерелах. Ми покажемо, що такі набори даних можуть формуватися за рахунок автоматичної побудови системи зв'язків між "стандартними" персональними даними.

Результати аналізу наукових публікацій. Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем саме по собі не є чимось новим. Мається на увазі правове регулювання відносин між людьми, які здійснюються за допомогою технологічних систем або у зв'язку з їх використанням.

При цьому виділяють дві основні категорії проблем:

- особливості функціонування технологічних систем як причина виникнення особливостей у додатковому правовому регулюванні;
- забезпечення захисту від наслідків нештатного функціонування технологічних систем.

Тобто суб'єктом права в будь-якому випадку є людина, а технологічна система виступає лише в ролі знаряддя в її руках. Отже, в ситуаціях, коли функціонування системи призводило до негативних наслідків, вважалося, що відповідальність за її дії несуть розробники, виробники та експлуатаційники, тобто люди.

Але сьогодні (принаймні, теоретично) розглядаються ситуації, в яких відповідальність може бути покладена саме на машину, незалежно від участі людини [2; 3]. Такий погляд на технологічні системи є принципово новим, оскільки передбачає можливість того, що їх функціонування може мати соціальні наслідки, а отже, вони самі можуть розглядатися як суб'єкти суспільних відносин. Фактично, сказане означає, що за певних умов технологічна система набуває елементів суб'єктності. На перший погляд, це суперечить загальноприйнятим уявленням про сутність технологічних систем. Адже вважається, що машина лише виконує програму, закладену в неї людиною. І разом з тим, розвиток сучасних інформаційних технологій, зокрема Інтернету речей, свідчить, що такі ситуації можливі. Якщо не вдаватися до наукової фантастики, то мова, очевидно, йде не про повноцінну суб'єктність машини, а про наявність в її функціонуванні окремих рис, характерних для справжнього суб'єкта – людини.

Вважаємо, що в рамках обраної нами теми ключовим чинником є здатність машини самостійно приймати рішення. Підкреслимо, що йдеться не про імітацію прийняття рішення, що, взагалі кажучи, на наш час не є чимось особливим (прикладом може служити комп'ютер, що грає в шахи). Ми маємо на увазі здатність машини приймати рішення, яке однозначно не визначається алгоритмом, обраними значеннями його параметрів та структурою вхідних даних. Саме така поведінка машини дає підстави говорити про її відповідальність за власні дії, що є предметом правового регулювання.

Загрози та ризики, що виникають в сфері використання IP, широко обговорюються в експертному середовищі. Стислий виклад поточного стану речей міститься, наприклад, в звітах групи Alliance for Internet of Things Innovation, (AIPI), створеної 2015 року у Європейській Комісії [9]:

- існуюча нормативно-правова база і регуляторні рамки, в основному, відповідають вимогам сучасного цифрового середовища;
- ключ до розвитку IP полягає у встановленні балансу між гарантуванням безпеки споживачів і стимулюванням інновацій;
- частина ризиків пов'язана з відповідальністю за якість продукції, якій надається особливе значення, хоча вона й застосовує IP, але це не є чимось унікальним для цієї продукції і платформ;

- виникають питання, пов’язані з відмінностями в поняттях “продукт” і “сервіс”, тому необхідні чіткі роз’яснення, щоб уникнути невизначеності;
- забезпечити такий розвиток регуляторної політики, щоб вона була досить гнучкою для можливості врахування схильності промисловості до постійного розвитку, що є для неї ключовим.

Окрему категорію становлять ризики, пов’язані з проблемою захисту персональних даних [7; 8; 10; 11]. ІР за своєю природою орієнтований на збирання великих обсягів даних. Серед них можуть бути і дані, які слід кваліфікувати як персональні.

Важливою є особливість систем ІР, яка полягає в тому, що активне використання великої кількості датчиків створює умови для формування комплексів даних, в тому числі і персональних [12].

Основні аспекти сучасної проблеми захисту персональних даних містяться, наприклад, в матеріалах звіту Федеральної торгової палати США [13]:

- переваги впровадження ІР зводяться до мінімуму наявністю негативних наслідків, наприклад, загрозами конфіденційності персональних даних;
- зайве регулювання в питаннях захисту персональних даних може призвести до уповільнення інвестицій в будь-який сектор;
- прийняття необхідного регулювання для гарантованого захисту персональних даних підвищить довіру споживачів до нових технологій;
- необхідно дочекатися проявів негативних наслідків і, тільки після цього, вживати заходів з регулювання;
- доцільно використовувати механізми саморегулювання замість регулювання законодавчими нормами.

Аналіз широкого кола джерел свідчить про те, що останнім часом проблема захисту персональних даних у використанні систем ІР активно переходить в сферу прийняття безпосередньо правових рішень [7; 8].

Метою статті є вивчення можливих механізмів генерації системами ІР з елементами штучного інтелекту наборів персональних даних, заснованих на використанні автоматично модифікованих алгоритмів..

Нижче ми проаналізуємо один із аспектів проблеми несанкціонованого поширення персональних даних системами ІР. А саме, принципову можливість системи ІР генерувати принципово нові набори персональних даних, засновану на використанні алгоритмів, що здійснюють агрегування вхідної інформації..

Виклад основного матеріалу. Перш за все зазначимо, що на наш час саме поняття персональних даних зазнало певного розширення в порівнянні з традиційним розумінням їх як “паспортні дані”. Відповідно до Загального регламенту про захист даних (GDPR), діючого в межах законодавства Європейського Союзу щодо захисту персональних даних, це поняття визначається як “…будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати” [14]. Аналогічно це поняття визначається і Законом України “Про захист персональних даних”.

Для нас в цьому визначенні важливі два моменти:

- персональними даними може бути будь-яка інформація;
- визначальним чинником є ідентифікованість відповідної особи, або принципова можливість такої ідентифікації.

Прийнято вважати, що персональні дані належать до одного з таких видів даних:

- літери;
- числа;

- графічні зображення (малюнки або картини);
- фото;
- аудіо;
- відео.

Також останнім часом до персональних відносять такі специфічні дані:

- файли cookies;
- IP-адреси.

Таким чином, персональні дані в сучасному розумінні мають досить широкий спектр.

Головна особливість маніпуляції персональними даними в системах ІР полягає в тому, що її здійснює машина, яка, взагалі кажучи, "не знає" який сенс мають ті або інші дані з точки зору людини. Саме ця особливість породжує специфічні ризики, зумовлені тим, що людині надзвичайно важко контролювати такі аспекти функціонування кібернетичних пристроїв.

На рівні технологічної реалізації ІР є набором датчиків, що фіксують задані параметри навколишнього середовища, та пристроїв, що обробляють вхідні дані, отримані від датчиків. Для нас суттєво, що обмін даними здійснюється за допомогою мережі Інтернет. Метою створення такої системи є виключення безпосередньої участі людини принаймні в частині функціональних можливостей системи. Це, в свою чергу означає, що система ІР повинна на основі обробки отриманих вхідних даних приймати рішення, результатом яких буде отримання додаткових даних. Ці додаткові дані можуть мати різні джерела, які більш чи менш строго розподіляються на дві групи:

- дані датчиків, які входять до складу відповідної системи ІР;
- дані, що знаходяться в мережі Інтернет, до якого дана система ІР має доступ.

Саме доступність даних другої групи може створювати складні неконтрольовані ситуації. Адже проектувальник системи не може передбачити, запит на які дані сформує машина в певній ситуації, навіть, якщо сама ситуація прогнозована.

Отримання машиною додаткових даних гіпотетично є актуальним для систем з елементами штучного інтелекту [1].

Поняття "штучний інтелект" є надзвичайно популярним і, разом з тим, доволі погано визначеним. В літературі з ним пов'язано багато різноманітних спекуляцій від технічних непорозумінь до відвертих фантазій в дусі футуризму та наукової фантастики. В дійсності існує дві основні точки зору на поняття "штучний інтелект":

- технологія створення обчислювальних машин, здатних вирішувати завдання, що традиційно вважаються інтелектуальними [15];
- властивість обчислювальних машин вирішувати такі завдання [16].

Головна складність полягає в тому, щоб строго визначити, які задачі слід вважати інтелектуальними. Зазвичай кажуть, що це задачі, що вимагають виконання творчих функцій, але саме поняття творчості також потребує строгого визначення. Яскравим прикладом можуть служити шахи. Чи слід віднести комп'ютерні програми гри в шахи до реалізації штучного інтелекту? З одного боку, шахи вважаються інтелектуальною грою, а з іншого – такі програми принципово не відрізняються від програм, скажімо, аналітичного розв'язання рівнянь. Спрощено кажучи, вони просто перебирають всі можливі ходи із заданою глибиною (n-ходів вперед) і кожному з них за допомогою деякого алгоритму привласнюють ваговий множник. Перевага віддається ходу з максимальною вагою. Ефективність програми визначається досконалістю алгоритму обчислення ваг, який розробляє людина, а не власне роботою машини.

В рамках пропонованого дослідження обмежимося однією з можливих реалізацій системи, поведінка якої може в розумному наближенні вважатися інтелектуальною. В основі її (реалізації) лежить поділ систем на лінійні і нелінійні. Поняття лінійності ми використовуємо в досить широкому сенсі. Саме, під лінійною ми будемо розуміти таку систему, для якої нескінченно малі відхилення вхідного сигналу призводять до нескінченно малих відхилень вихідного сигналу. Відповідно, нескінченно мале відхилення вхідного сигналу нелінійної системи призводить до кінцевого відхилення вихідного сигналу. А це означає, що при нескінченно малих (і тому непомітних для нас) збуреннях даних, які машина так чи інакше отримує на вході, вона може виконувати дії, що не збігаються з тими, які повинні відбутися при незбурених значеннях цих даних. І тут мова не йде про імітацію інтелектуальної діяльності: машина дійсно веде себе самостійно з нашої точки зору, оскільки кінцевий результат не належить до наперед заданого набору можливих варіантів.

Таким чином, під штучним інтелектом ми розумітимемо технологію створення обчислювального комплексу, що представляє собою деяку нелінійну систему. Відзначимо, що мова йде про нелінійність всього комплексу, а не тільки програми, оскільки істотну роль можуть грати механізми отримання вхідних даних.

Безпосередньо нас цікавить ситуація, в якій машина використовує персональні дані, не передбачені при її створенні. В "звичайних" кібернетичних системах такі ситуації не виникають. Кожний конкретний програмно-апаратний комплекс від початку призначений для обробки певного набору даних, серед яких можуть бути і персональні. Процеси несанкціонованого збирання та поширення персональних даних є доволі простими і зрозумілими. Ми розуміємо їх причини і механізми. Проблема полягає лише в тому, щоб віднайти адекватні засоби відповідних дій.

Зовсім інший стан справ виникає тоді, коли машина здатна сама генерувати персональні дані, використовуючи інші дані, на перший погляд такі, що не мають відношення до персональних. При цьому, очевидно, так чи інакше машина повинна використовувати додаткові дані, які вона збирає самостійно, використовуючи алгоритми власного виробництва (наприклад, в рамках можливості самонавчання). Джерелами таких даних, звичайно, можуть бути і власні датчики системи ІР, і доступні для неї ресурси мережі Інтернет.

З точки зору проектувальників, відповідна система ІР може взагалі не оперувати персональними даними, або оперувати ними в обмежених рамках. Але ми вже казали, що до персональних даних можуть бути віднесені будь-які відомості, так чи інакше пов'язані з тією чи іншою особою. І вони можуть складатися з кількох компонентів. Частина з них передбачена штатним режимом експлуатації системи, а частина – збирається і обробляється машиною в рамках використання модифікованих алгоритмів.

Наведемо умовний (гіпотетичний) приклад, який ілюструє сказане вище. Нехай маємо систему ІР категорії "розумний будинок" (мається на увазі технологія керування різноманітними побутовими приладами, а також здійснення різноманітних видів віддаленого моніторингу, дані яких визначають прийняття рішень в конкретних ситуаціях). Шляхом вдосконалення алгоритмів, що керують засобами охорони будинку, система фіксує людину, яка наближається на критичну відстань, ідентифікує її за обличчям, а потім здійснює пошук в доступних базах на предмет реєстрації її як терориста, педофіла тощо. При цьому машина може завантажувати вміст баз даних, які містять дані на цю людину, створюючи її власний профіль. Оскільки такі дані машина використовує сама, ми можемо не мати про це жодного уявлення. Але за певних умов ці

дані можуть бути кимось використані або відповідно до характеру роботи машини, або внаслідок зламу системи сторонніми особами.

Такі ситуації породжують додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина.

Висновки.

Отже, ми бачимо, що за певних умов характер взаємодії ІР з оточуючим середовищем може призводити до нелінійних ефектів з елементами непередбачуваної поведінки системи. Один із можливих випадків пов'язаний з використанням машиною непередбачених наборів даних, серед яких можуть бути присутні і персональні дані.

Ми бачимо, що системи ІР з елементами штучного інтелекту в процесі експлуатації в принципі здатні розширювати штатний режим отримання та обробки даних, внаслідок чого машина стає здатна самостійно генерувати персональні дані, використовуючи інші дані, отримані в передбачений спосіб. При цьому машина так чи інакше повинна використовувати додаткові дані, які вона збирає самостійно, використовуючи модифіковані алгоритми (наприклад, в рамках можливості самонавчання). Джерелами таких даних, звичайно, можуть бути і власні датчики системи ІР, і доступні для неї ресурси мережі Інтернет.

В результаті виникають додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. Отже, виникає необхідність врахування таких загроз при розробці норм законодавства щодо захисту персональних даних, а також адекватних механізмів реалізації цих норм на практиці.

Використана література

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования: збірник матеріалів ІІ-ї Міжнародної науково-практичної конференції *"ІТ-право: проблеми та перспективи розвитку в Україні"*, м. Львів, 17 листопада 2017 р. Львів: НУ "Львівська політехніка", 2017. 318 с. С. 18-42.

2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений. – Структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: http://handle.itu.int/11.1002/1000/11559

3. Баранов О.А. "Інтернет речей" як правовий термін. *Юридична Україна*. 2016. № 5-6. С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21C OM=2&I21 DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr _2016_5-6_16.pdf

4. Леонид Черняк. Платформа Интернета вещей (рус.). *Открытые системы. СУБД*. 2012. № 7, URL: https://www.osp.ru/os/2012/07/13017643

5. Kevin Ashton. That 'Internet of Things'. In the real world, things matter more than ideas. (англ.). RFID Journal (22 June 2009) http://www.rfidjournal.com/articles/view?4986

6. 'Internet of Things' (англ.). Gartner IT glossary. Gartner (5 May 2012). – 'The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment'. URL: https://www.gartner.com/it-glossary/internet-of-things

7. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. *Інформація і право*. № 2(17)/2016. С. 85-91. URL: http://ippi.org.ua/sites/default/files/11_0.pdf

8. Брижка В.М. , Пилипчук В.Г. та ін. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

9. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels, 28 October 2015. URL: http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels

10. Интернет вещей: чем угрожает будущее. URL: http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee

11. Как в 2015 году был взломан Интернет вещей. URL: http://igate.com.ua/ news/12342-kak-v-2015-godu-byl-vzloman-internet-veshhej

12. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protectionof individuals with regard to automatic processing of personal data in the context of profiling (Adopted by theCommittee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). URL: https://search.coe.int/cm/Pages/result_details.aspx? ObjectID=09000016805cdd00

13. Internet of Things: Privacy & Security in a Connected. World Federal Trade Commission (FTC) Staff Report. January 2015. URL: https://www.ftc.gov/system/files/documents /reports/ federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrpt.pdf

14. Регламент (ЄС) 2016/679 від 27.04.16 р. "Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальний Регламент про захист даних)". URL: https://gdpr-text.com/?col =2&lang1 =ukr&lang2=en&lang3=rumain. – (Переклад Регламенту та ін. правових стандартів ЄС надано у кн.: *Сучасні правові стандарти Євросоюзу у сфері захисту персональних даних* / [І. Майстренко – пер. з англ.; В. Брижко – ред. тексту]. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 177 с.).

15. What is Artificial Intelligence? FAQ от Джона Маккарти, 2007. URL: http://www-formal.stanford.edu/jmc/whatisai/whatisai.html

16. Аверкин А.Н., Гаазе-Рапопорт М.Г., Поспелов Д.А. Толковый словарь по искусственному интеллекту. Москва: Радио и связь, 1992. 256 с. URL:http://www.raai.org/library/tolk/aivoc.html#L208

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

УДК 346.3:004(477)

МАНЬГОРА В.В., *кандидат педагогічних наук, доцент,*
професор кафедри права "ПрАТ "ВНЗ "МАУП"

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЕЛЕКТРОННИХ ГОСПОДАРСЬКИХ ДОГОВОРІВ В УКРАЇНІ

Анотація. *В статті досліджуються особливості правого регулювання електронних господарських договорів на сучасному етапі в Україні. Здійснено аналіз чинного законодавства що регулює електронні господарські договори в Україні. Проаналізовано різні точки зору щодо форми електронних договорів в сучасній правовій науці. Визначено основні проблеми правового регулювання господарських електронних договорів. Розроблено пропозиції щодо вдосконалення чинного законодавства що регулює електронні господарські договори в Україні.*

Ключові слова: *електронні господарські договори, електронні довірчі послуги, електронна комерція, форма електронних договорів.*

Summary. *The article explores the features of the legal regulation of electronic business agreements at the present stage in Ukraine. The current legislation governing electronic business agreements in Ukraine has been analyzed. Different perspectives on the form of electronic contracts in modern legal science have been analyzed. The main problems of legal regulation of business electronic agreements are identified. Proposals have been made to improve the current legislation governing electronic business agreements in Ukraine.*

Keywords: *electronic business agreeements, electronic trust services, e-commerce, a form of electronic contracts.*

Аннотация. *В статье исследуются особенности правового регулирования электронных хозяйственных договоров на современном этапе в Украине. Осуществлен анализ действующего законодательства, регулирующего электронные хозяйственные договоры в Украине. Проанализированы различные точки зрения относительно формы электронных договоров в современной правовой науке. Определены основные проблемы правового регулирования хозяйственных электронных договоров. Разработаны предложения по совершенствованию действующего законодательства, регулирующего электронные хозяйственные договоры в Украине.*

Ключевые слова: *электронные хозяйственные договоры, электронные доверительные услуги, электронная коммерция, форма электронных договоров.*

Постановка проблеми. Розвиток торгівлі, збуту промислової продукції, постачання господарюючим суб'єктам необхідної сировини, матеріалів й устаткування, надання фізичним і юридичним особам різноманітних послуг у сфері обслуговування потребує регулювання договірних відносин, господарський договір є основним правовим документом, який регулює відносини сторін, учасників господарських правовідносин та є однією з основних підстав виникнення господарських зобов'язань.

За сучасних умов інформаційні відносини набувають дедалі більшої ваги і стають одними із найважливіших елементів розвитку господарсько-правових відносин, одним із видів яких є договірні відносини. Розвиток комп'ютерної мережі Інтернет, електронної торгівлі призводить до збільшення кількості електронних господарських договорів.

Виникнення нових правовідносин потребує прийняття нових нормативно-правових актів, внесення змін щодо чинних, враховуючи досвід інших країн, рекомендації міжнародних організацій та експертів, судової практики.

Результати аналізу наукових публікацій. Проблемі правого регулювання електронних господарських договорів були присвячені праці таких авторів, як А. Воронової [1], Є. Дробиш [2], С. Жуткової [3], Н. Кучаковської [4], А. Чучковської [5], А. Шумило [6].

Метою статті є визначення особливостей правого регулювання електронних господарських договорів в Україні, виявлення основних проблем застосування електронних господарських договорів та розробка пропозицій щодо вдосконалення чинного законодавства, що регулює електронні господарські договори.

Виклад основного матеріалу. З метою удосконалення нормативно-правового регулювання електронного документообігу з метою наближення умов його застосування до документообігу на паперових носіях Верховна Рада України прийняла Закон України "Про електронні довірчі послуги" від 5 жовтня 2017 р. [7], Закон України "Про електронний цифровий підпис" втратив чинність [8].

Закон України "Про електронні довірчі послуги" набув чинності від 7 листопада 2018 р. та передбачає: якщо відповідно до законодавства на паперовому документі не потрібен власноручний підпис сторін, при електронному документообігу можна використовувати електронні дані або ж ні – за домовленістю сторін.

Основними законодавчими актами, що регулюють відносини щодо електронних договірних відносин в господарюванні, є Господарський кодекс України від 16 січня 2003 р., Цивільний кодекс України від 16 січня 2003 р. та Закон України "Про електронну комерцію" від 26 квітня 2017 р.

Відповідно до п. 5 ч. 1 ст. 5 Закону України "Про електронну комерцію" електронний договір – домовленість двох або більше сторін, спрямована на встановлення, зміну або припинення цивільних прав і обов'язків та оформлена в електронній формі [9].

В сучасні правовій науці існують різні точки зору щодо форми електронних договорів. Одні поділяють думку західних вчених, що електронна форма правочину є окремою формою правочину. На думку представників іншої позиції, зокрема І. Спасибо-Фатєєвої, А. Чучковської та О. Гудзь, правочин, вчинений з використанням електронних засобів зв'язку, є різновидом письмової форми [4, с. 876].

Згідно з ч. 1 ст. 181 Господарського кодексу України господарський договір за загальним правилом викладається у формі єдиного документа, підписаного сторонами та скріпленого печатками. Допускається укладення господарських договорів у спрощений спосіб, тобто шляхом обміну листами, факсограмами, телеграмами, телефонограмами тощо, а також шляхом підтвердження прийняття до виконання замовлень, якщо законом не встановлено спеціальні вимоги до форми та порядку укладення даного виду договорів [10].

Закон України "Про електронну комерцію" доповнив частину другу статті 639 Цивільного кодексу України абзацом другим такого змісту: "Якщо сторони домовилися укласти договір за допомогою інформаційно-телекомунікаційних систем, він вважається укладеним у письмовій формі". Відповідно до ст. 205 Цивільного кодексу України правочин може вчинятися усно або в письмовій (електронній) формі. Стаття 207 Цивільного кодексу України визначає, що правочин вважається таким, що вчинений у письмовій формі, якщо його зміст зафіксований в одному або кількох документах (у тому числі електронних), у листах, телеграмах, якими обмінялися сторони [11]. Отже, Господарський кодекс України та Цивільний кодекс України, визначають, що договори, укладені в електронній формі, є такими, що укладені у письмовій формі. Проте, на нашу думку, потрібно електронні договори винести в окрему групу договорів, так як вони

мають свої особливості укладання і відрізняються від усних та письмових договорів. Вирішення даної проблеми буде зумовлено правозастосовною практикою, яка вимагає чіткого механізму регулювання господарських електронних договорів при вирішені питань щодо спорів між особами, що уклали електронний договір.

При укладенні електронних господарських договорів є важливим, те що він має включати всі істотні умови, якщо ні, то він може бути визнаний неукладеним або недійсним відповідно до ч. 1 ст. 638 Цивільного кодексу України, Договір є укладеним, якщо сторони в належній формі досягли згоди з усіх істотних умов договору. Істотними умовами договору є умови про предмет договору, умови, що визначені законом як істотні або є необхідними для договорів даного виду, а також усі ті умови, щодо яких за заявою хоча б однієї із сторін має бути досягнуто згоди [12].

Відповідно до ст. 11 Закону України "Про електронну комерцію" електронний договір, крім визначених Цивільним кодексом України істотних умов для відповідного виду договору, може містити інформацію про:

- технологію (порядок) укладення договору;
- порядок створення та накладання електронних підписів сторонами договору;
- можливість та порядок внесення змін до умов договору;
- спосіб та порядок прийняття пропозиції укласти електронний договір (акцепту);
- порядок обміну електронними повідомленнями та інформацією між сторонами під час виконання ними своїх зобов'язань;
- технічні засоби ідентифікації сторони;
- порядок внесення змін до помилково відправленого прийняття пропозиції укласти електронний договір (акцепту);
- посилання на умови, що включаються до договору, шляхом перенаправлення (відсилання) до іншого електронного документа і порядок доступу до такого документа;
- спосіб зберігання та пред'явлення електронних документів, повідомлень, іншої інформації в електронній формі та умови доступу до них;
- умови виготовлення та отримання паперових копій електронних документів;
- можливість вибору мови, що використовується під час укладення та виконання договору;
- інші відомості [9].

Сторони електронних господарських договорів мають розуміти у яких випадках потрібно укладати електронний договір, а яких укладати у вигляді письмової форми, або використовувати інші засоби електронної комунікації.

Основними проблемами правового регулювання господарських електронних договорів, на нашу думку є:

- ідентифікація суб'єктів;
- вибір необхідних технологій ідентифікації;
- підтвердження цілісності даних в електронній формі.

Якщо форма договору – електронна, то й ідентифікація буде електронною.

Якщо договір укладається в домовленостях електронною поштою – воля сторін буде виражена в змісті такого листування. Якщо ж домовленість формується як приєднання до договору – підписання та ідентифікація можлива в декілька способів:

1. Електронний підпис під час заповнення стандартної форми. Споживач вносить свої дані, за необхідності – завантажує скан-копії документів, а потім натискає кнопку "погодитись". Договір вважатиметься укладеним в електронній формі.

2. Одноразовим ідентифікатором. Це пароль, який система надсилає вам на телефон або електронну пошту для підтвердження вашої згоди на проведення операції,

або ж шляхом реєстрації в якості користувача на веб-ресурсі (коли в якості ідентифікатора у вас будуть власні логін та пароль).

3. Факсимільного підпису. Використовується, якщо у сторін є аналоги власноручних підписів, проте фактично майже не застосовується, оскільки фактичного підписанта буде складно ідентифікувати.

4. Електронного цифрового підпису. Цей спосіб застосовується, якщо угода оформлюється у вигляді окремого документу. На документ накладається підпис із використанням кодового ключа, що дозволяє перевірити і встановити підписанта.

На думку Є. Дробиш в будь-якому випадку, не зважаючи на обрану модель, в договорі варто прописати, за яких умов згода щодо його умов вважатиметься досягнутою, а договір – підписаним [2].

Відповідно до ст. 1 Закону України "Про електронні довірчі послуги" визначено, що електронний підпис – це електронні дані, які додаються підписантом до інших електронних даних або логічно з ними пов'язуються і використовуються ним як підпис [7].

Кваліфікований електронний підпис має таку саму юридичну силу, як і власноручний підпис, та має презумпцію його відповідності власноручному підпису. Електронний підпис чи печатка не можуть бути визнані недійсними та позбавлені можливості розглядатися як доказ у судових справах виключно на тій підставі, що вони мають електронний вигляд або не відповідають вимогам до кваліфікованого електронного підпису чи печатки [6].

Використання електронного цифрового підпису має певні переваги для суб'єктів господарювання, – це додаткові можливості шифрування документів, які забезпечать конфіденційність інформації. Укладення електронних господарських договорів сприяє економії часу підприємців. Використання електронних господарських договорів є досить поширеним в інших країнах, що вимагає від вітчизняних компаній все частішого застосування даної форми договорів.

Висновки.

Отже, прийняття Законів України "Про електронну комерцію" та "Про електронні довірчі послуги", внесення змін до діючих нормативно-правових актів значно розширило б можливості суб'єктів господарювання використовувати в своїй діяльності електронні господарські договори. Проте, інформаційно-телекомунікаційні системи постійно розвиваються і потребують прийняття нових підзаконних нормативно-правових актів для повноцінного впровадження вказаних вище законів та внесення змін до них.

Винесення електронних договорів в окрему групу договорів передбачає внесення змін до Цивільного кодексу України. Для цього необхідно ч. 1 ст. 205 Цивільного кодексу України викласти в такій редакції: Правочин може вчинятися усно, в письмовій, електронній формі. Сторони мають право обирати форму правочину, якщо інше не встановлено законом.

Виділення електронних договорів в окрему форму дасть можливість чітко визначити істотні умови договору, зменшить кількість випадків коли договір визнається неукладеним або недійсним.

Використана література

1. Воронова А. Изменения в договорной практике после принятия Закона "Об электронной коммерции". – (Материал аналитического изд. ЮРИСТ&ЗАКОН № 31 от 1 сентяб. 2016 г.). URL: http://jurliga.ligazakon.ua/news/2016/9/2/149923.htm

2. Дробиш Є.Д. Електронні договори: питання оформлення і підписання. URL: https://www.uvito.ua/blog/elektronni-dogovori-pitannya-oformlennya-i-pidpisannya

3. Жуткова С.М. Особливості укладання угод через мережу Інтернет. *Молодий вчений*. 2017. № 11(51). С. 875-879.

4. Кучаковська Н. Правове регулювання укладення електронних господарських договорів. *Зовнішня торгівля: економіка, фінанси, право*. 2016. № 6. С. 62-74.

5. Чучковська А. Форма господарських договорів, що вчиняється через мережі електрозв'язку, зокрема через Інтернет. *Підприємництво, господарство і право*. 2003. № 12. С. 8-11.

6. Шумило А. Електронні договори: особливості користування URL: http://mbusines spartner.com.ua/elektronni-dohovory

7. Про електронні довірчі послуги: Закон України від 05.10.17 р. № 2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.

8. Про електронний цифровий підпис: Закон України від 22.05.03 р. *Відомості Верховної Ради України*. 2003. № 36. Ст. 236.

9. Про електронну комерцію: Закон України від 03.09.15 р. № 675-VIII. *Відомості Верховної Ради України*. 2015. № 45. Ст. 410.

10. Господарський кодекс України: Закон України від 16.01.03 р. № 436-IV. *Відомості Верховної Ради України*. 2003. № 18. № 19-20, № 21-22. Ст. 144.

11. Цивільний кодекс України: Закон України від 16.01.03 р. № 435-IV *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356.

12. Електронний договір і порядок його підписання URL: https://protocol.ua/ua/elek tronniy_dogovir_i_poryadok_yogo_pidpisannya

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Інформаційна і національна безпека

УДК 340+35.078.3

ТАРАСЮК А.В., *кандидат юридичних наук,*
НДІ інформатики і права НАПрН України

СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Анотація. *У статті досліджується концептуальні засади співвідношення інформаційної та кібернетичної безпеки України. На основі теоретичного аналізу запропоновано авторські визначення базових категорій кібернетичної безпеки, а також визначено та проаналізовано стан законодавчого забезпечення та розроблено пріоритетні напрями його вдосконалення.*

Ключові слова: *інформаційна безпека України, забезпечення інформаційної безпеки, кібербезпека, загроза.*

Summary. *The article explores the conceptual principles of information and cyber security of Ukraine. On the basis of theoretical analysis, author's definitions of basic categories of cyber security have been proposed, as well as the state of legislative support has been determined and analyzed and priority directions for its improvement have been developed.*

Keywords: *information security of Ukraine, information security, cyber security, threat.*

Аннотация. *В статье исследуются концептуальные основы соотношения информационной и кибернетической безопасности Украины. На основе теоретического анализа предложены авторские определения базовых категорий кибернетической безопасности, а также определено и проанализировано состояние законодательного обеспечения и разработаны приоритетные направления его совершенствования.*

Ключевые слова: *информационная безопасность Украины, обеспечение информационной безопасности, кибербезопасность, угроза.*

Постановка проблеми. Цілком очевидно, що й сьогоднішні, й перспективні, адекватні соціальній дійсності наукові розвідки у сфері інформаційної безпеки без опори на класичну спадщину будуть досить сумнівними. Водночас, не менш очевидно, що творчість найвидатніших представників світової філософської думки, незважаючи на її беззаперечну цінність і неминущу актуальність, далеко не вичерпує усіх аспектів філософського осягнення проблеми кібербезпеки.

А прецінь, їх погляди є найбільш показовими як у своїй протилежності, так і в єдності, що може стати тим перспективним аспектом осмислення сутності кібербезпеки, навколо якого й будуватиметься майбутня система забезпечення інформаційної безпеки як на національному, так і на глобальному рівнях. Принаймні сучасні методологічні підходи до соціально-філософського аналізу феномена інформаційної безпеки мають увібрати в себе якомога більше позитивних елементів проаналізованої історичної спадщини. Ретроспективний аналіз даної проблеми потрібен для вибору перспективної методології дослідження питань кібербезпеки України.

Нині у глобальному медіапросторі, в публіцистичних і наукових працях, а також у політичних і державних документах багатьох країн широкого вжитку набули терміни “інформаційна війна”, “інформаційне протиборство”, “інформаційний вплив”, “інформаційна зброя” тощо. Інформаційно-комунікаційні технології (далі – ІКТ) відіграють ключову роль у світовій політиці, економіці та системах безпеки.

До інформаційних диверсій у кіберпросторі сьогодні вдаються як організовані групи, так і окремі особи. Дедалі важливішою складовою військового потенціалу держав стає інформаційна зброя (далі – ІЗ) як доповнення до власне військового арсеналу. При цьому за своїми наслідками інформаційні війни між державами можуть бути не менш руйнівними і жорстокими, ніж традиційні.

Результати аналізу наукових публікацій. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроекти, які стосуються предмету дослідження, а також творчий доробок відомих вчених, зокрема В. Білоуса, В. Брижка, О. Довганя, І. Дороніна, Є. Захарова, М. Присяжнюка, В. Рубана, Т. Ткачука, В. Фурашева та ін.

Метою статті є визначення концептуальних засад правового співвідношення інформаційної та кібернетичної безпеки з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. Сьогодення постає перед Україною з новими викликами та надскладними завданнями. Під час опору різноплановим проявам гібридної війни, розгорнутої Російською Федерацією, стало очевидним, що наразі наша держава стикнулася з життєвою необхідністю захисту фундаментальних національних цінностей – незалежності, територіальної цілісності й суверенітету держави, свободи, прав людини й верховенства права, добробуту, миру й безпеки, – а також у стислі терміни має забезпечити ефективне функціонування сектору безпеки й оборони в умовах обмежених ресурсів. Запорукою успішної протидії широкомасштабній зовнішній агресії та сталого розвитку інформаційного суспільства в Україні є сьогодні не лише нарощування технологічних можливостей здійснення інформаційного обміну, а й глибоке усвідомлення усіма суб'єктами інформаційних відносин необхідності здійснення усіх заходів захисту інформаційних ресурсів та забезпечення інформаційної безпеки держави [1, с. 45-46], що неможливо без чіткого усвідомлення сутності останньої. Цікавим є й той факт, що самі російські дослідники відзначають, що інформаційна безпека від другої половині XX сторіччя стає одним із найважливіших елементів національної безпеки.

Стаття 17 Конституції України визначає, що "захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу" [2], що свідчить про набуття категорією "інформаційна безпека" в нормативно-правовому аспекті конституційного статусу [3, с. 30].

Незважаючи на те, що напрямок наукових досліджень, предметом якого є питання інформаційної безпеки, почав формуватись у період інтенсивної інформатизації, саме це явище існує стільки ж, скільки існує людство, дістаючи прояву в усіх сферах життєдіяльності суспільства. В повсякденному житті під інформаційною безпекою розуміють зазвичай необхідність протидії витоку інформації з обмеженим доступом, а також поширенню недостовірної інформації, однак застосування системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від побутового [4, с. 174].

Зауважимо, що система інформаційної безпеки, особливо на рівні її вихідних компонентів, може бути структурована за різними критеріями. Щодо кібернетичної безпеки, то Законом України "Про основні засади забезпечення кібербезпеки України" [5] вона визначена як "захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного

середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі". Виокремлення кібербезпеки зумовлене специфікою середовища, у якому функціонують інформаційні системи, здійснюється обіг інформації, реалізації законних інтересів суб'єктів інформаційних процесів. Тож "кібернетичний вимір" властивий усім складовим інформаційної безпеки. Варто зауважити, що кібербезпека нами розглядається як складова інформаційної безпеки Далі на Рис. представлено співвідношення інформаційної та кібернетичної безпеки.

Саме прийняття Закону України "Про основні засади забезпечення кібербезпеки України" означає для України закріплення на законодавчому рівні понятійного апарату з приставкою "кібер" і початок регулювання цифрової економіки в цілому.

Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої указом президента у 2016 році. Метою стратегії було створення умов для безпечного функціонування кіберпростору, його використання в інтересах особистості, суспільства і держави. При цьому основний масив положень стратегії стосується сфери національної оборони і не зачіпає бізнес. Стратегія стала підтвердженням прийнятого Україною курсу на євроінтеграцію, початком якого було підписання і ратифікація Україною Конвенції про кібербезпеку. Держави-члени Ради Європи та деякі інші держави, які підписали конвенцію, взяли на себе зобов'язання ужити загальних та індивідуальних заходів для запобігання злочинам у цифровій сфері.

Основним досягненням Закону "Про основні засади забезпечення кібербезпеки України" є імплементація в правове поле визначень, що стосуються кібербезпеки, кібератак і кіберзахисту.

Не вдаючись в детальний аналіз вказаного Закону, відзначимо ряд принципово важливих, на нашу думку, дискусійних аспектів, які у перспективі слід буде доопрацьовувати та вдосконалювати:

- чи поширюється Закон на приватні мережі суб'єктів господарювання, адже такі мережі, все ж таки підключені до мережі Інтернет;

- неузгодженість та відсутність конкретизації повноважень суб'єктів національної системи кібербезпеки;

- декларативний зміст ряду положень, що потребує прийняття цілого ряду конкретизуючих підзаконних нормативно-правових актів.

Крім практичної площини та зважаючи на відсутність єдності науковців щодо місця кібербезпеки у системі інформаційної безпеки, запропонуємо авторське розуміння її основних складових, а також її співвідношення з інформаційною безпекою держави.

Кібернетичний, або *спеціальний програмно-математичний вплив* реалізується з використанням засобів знищення, перекручення або розкрадання інформаційних масивів. Після подолання систем захисту противника з його інформаційних масивів отримується інформація, володіння якою вважається необхідним; доступ до них для законних користувачів при цьому обмежується чи взагалі унеможливлюється. У рамках кібервпливу вдаються також до дезорганізації роботи технічних засобів, виведення з ладу телекомунікаційних мереж, комп'ютерних систем тощо [6, с. 132-133].

Кібервплив провадять у *кібернетичному просторі* (кіберпросторі), під яким розуміють сферу діяльності в інформаційному просторі, утворену сукупністю комунікаційних каналів мережі Інтернет та інших телекомунікаційних мереж, технологічної інфраструктури, що забезпечує їх функціонування, і будь-яких форм здійснюваної за їх допомогою людської активності (окремого індивіда, організації, держави тощо).

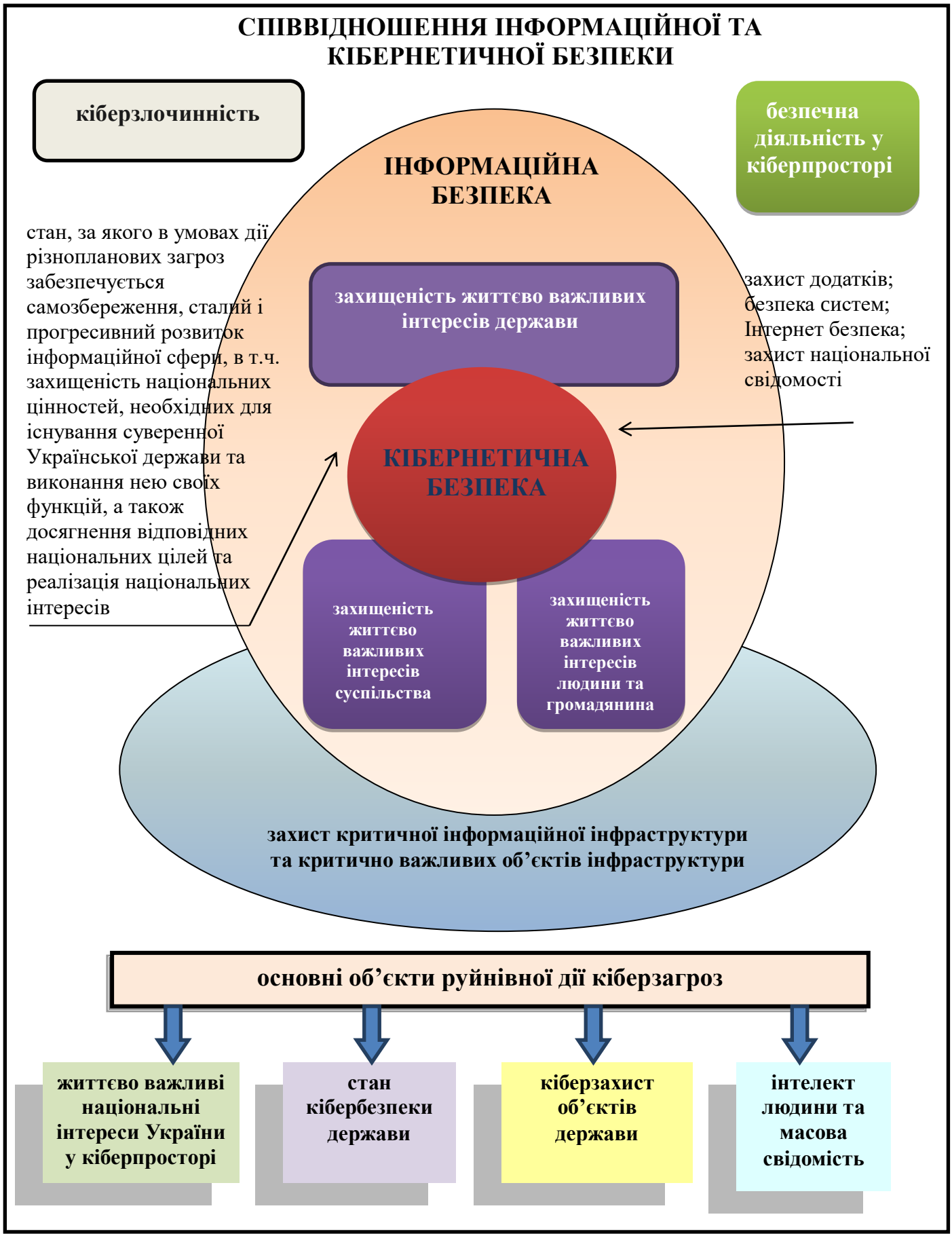

СПІВВІДНОШЕННЯ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ
кіберзлочинність
безпечна діяльність у кіберпросторі
ІНФОРМАЦІЙНА БЕЗПЕКА
стан, за якого в умовах дії різнопланових загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, в т.ч. захищеність національних цінностей, необхідних для існування суверенної Української держави та виконання нею своїх функцій, а також досягнення відповідних національних цілей та реалізація національних інтересів
захищеність життєво важливих інтересів держави
захист додатків; безпека систем; Інтернет безпека; захист національної свідомості
КІБЕРНЕТИЧНА БЕЗПЕКА
захищеність життєво важливих інтересів суспільства
захищеність життєво важливих інтересів людини та громадянина
захист критичної інформаційної інфраструктури та критично важливих об'єктів інфраструктури
основні об'єкти руйнівної дії кіберзагроз
життєво важливі національні інтереси України у кіберпросторі
стан кібербезпеки держави
кіберзахист об'єктів держави
інтелект людини та масова свідомість

Рис.

Кіберзагрози, або *інформаційно-технічні загрози*, хоча і є відносно новим видом інформаційних загроз, становлять суттєву небезпеку, серед іншого й через доволі швидкі темпи розвитку цього напряму. За сферами впливу кіберзагрози класифікують на дві групи. Перша з них пов'язана з атаками на бізнес і включає комерційне шпигунство, крадіжки баз даних, інформаційні дії з метою завдання шкоди репутаційному капіталу і т. ін. У разі подібних атак хакерам протистоять комп'ютерні фахівці корпорацій, кіберспецслужби. Якщо йдеться про кіберзагрози другої групи, то вони спрямовані на пристрої, що забезпечують життєдіяльність суспільства, контролюють пересування, роботу великої кількості служб і мають на меті злам комп'ютерних систем, крадіжку даних, нелегальне набуття можливості безкоштовно користуватися різними сервісами, видалення і зміну інформації про себе, свою (або замовника) активність і т. ін.

У Європейській Конвенції з кібернетичних злочинів наведено таке визначення цього поняття: *кіберзлочини – це правопорушення, спрямовані проти конфіденційності, цілісності та доступності комп'ютерних систем, мереж і даних, а також їх неправомірне використання* [7]. Віртуальний характер кіберзлочинів, а також засоби, за допомогою яких вони здійснюються, дозволяє зловмисникам швидко знищити сліди. Це значно ускладнює з'ясування обставин і пошук винуватців, тож постає нагальна потреба в розробленні нових методів розслідування кіберзлочинів і відповідних законодавчих норм, що регламентують сферу інформаційної безпеки.

Таким чином, на сучасному етапі бойові дії ведуться і в *інформаційному просторі* – принципово новому середовищі, де формується, перетворюється, передається, використовується, зберігається інформація, що впливає на індивідуальну і суспільну свідомість, інформаційну інфраструктуру і власне інформацію. Можна констатувати наявність не лише інформаційного простору як частини загального геостратегічного ландшафту, а й передумов для створення, розвитку й поширення інформаційної зброї. З огляду на це збройні конфлікти дедалі більше тяжіють до формату багатовимірних інформаційних війн і можуть одночасно вестися на різних рівнях. Термін "інформаційна війна" вперше був офіційно застосований у документах Міністерства оборони США. в директиві МО США DODD 3600 від 21 грудня 1992 року [8, с. 6-7].

В інформаційно-технічному протиборстві головними об'єктами нападу і захисту є системи управління та зв'язку, телекомунікаційні системи, радіоелектронні засоби, а також інформаційні ресурси держави – інформація на матеріальних носіях або наявна в будь-який інший формі. Саме в цій сфері сформувалося поняття ІЗ як *сукупності засобів розвідки, управління, зв'язку, навігації та радіоелектронної боротьби*. Загальновживаним термін "інформаційна зброя" став після завершення військової операції "Буря в пустелі" (Ірак, 1991), у ході якої комплексне застосування вищенаведеного переліку засобів на театрі військових дій зіграло вирішальну роль у досягненні стратегічної мети [6, с . 22-23].

Інформаційно-комунікаційні технології є одним з найбільш важливих факторів, що впливають на формування суспільства XXI століття, – зазначається в Окінавській Хартії глобального інформаційного суспільства. Їх революційний вплив стосується способу життя людей, їх освіти і роботи, а також взаємодії уряду та громадянського суспільства. Інформаційні технології швидко стають життєво важливим стимулом розвитку світової економіки [9]. Відповідно міжнародне законодавство останнім часом почало приділяти значну увагу кіберзагрозам та протидії їм.

Серед основних загроз національним кіберпросторам стратегії більшості країн визначають:

- *Кібершпигунство та військові дії, які здійснюються за підтримки або з відома*

держави. Усі технологічно розвинені держави та корпорації стають об'єктом кібершпигнуства, яке має на меті заволодіння державними або промисловими таємницями, персональними даними або іншою цінною інформацією [10]. Так, однією з найрезонансніших кібератак за останній час стали дії КНДР проти компанії "Sony Pictures Entertainment", внаслідок яких зловмисники заволоділи конфіденційними даними, в тому числі інформацією про комерційні операції компанії [11].

- *Використання Інтернету у терористичних цілях*. Терористичні угрупування використовують Інтернет з метою пропаганди, збору коштів і вербування прихильників [10].
- *Кіберзлочинність: викрадення персональних даних та відмивання коштів, отриманих незаконним шляхом*. Зловмисники продають інформацію про номери банківських карток, паролі від комп'ютерних серверів та шкідливе ПЗ.

Відповідно, національні законодавства країн, як правило, регулюють питання захисту:

- персональних даних (Канада, Нідерланди, Естонія, Швеція, Фінляндія, Іспанія);
- електронної комерції та безпеки електронних транзакцій та платіжних інструментів (США, Канада, Польща, Естонія, Італія);
- дітей (США);
- важливих об'єктів інфраструктури та інформаційних систем (Франція) [12, с. 244].

По-різному й трактують поняття "кібербезпека" в зарубіжних країнах:

– сукупність організаційних, правових, технічних та освітніх заходів, спрямованих на забезпечення безперервного функціонування кіберпростору (*Політика захисту кіберпростору Республіки Польща*).

– бажаний стан безпеки інформаційних технологій, за якого ризики для кіберпростору скорочені до прийнятного мінімуму (*Стратегія кібербезпеки Німеччини*).

– заходи з попередження шкоди від збоїв в роботі ІКТ та в її усуненні (*Національна стратегія кібербезпеки Королівства Нідерланди*).

– бажаний стан інформаційної системи, за якого вона може протидіяти викликам кіберпростору, які можуть негативно вплинути на достовірність, цілісність та конфіденційність даних, що зберігаються або обробляються даною системою (*Стратегія безпеки та оборони інформаційних систем Франції*) [13, с. 143].

Щодо вітчизняного правового регулювання окреслених питань, на законодавчому рівні системи інформаційної безпеки досі комплексно не вирішено. Навіть нова Доктрина інформаційної безпеки України [14], яка готувалася в умовах, коли наша країна потерпає від гібридної агресії Російської Федерації, а отже – вже треба було б усвідомлювати значення інформації, інформаційних впливів та інформаційної сфери в цілому, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

Так, виходячи з необхідності вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері, з початком гібридної війни проти України виникла необхідність кардинальних змін у системі забезпечення інформаційної безпеки нашої держави. Основний план заходів було запроваджено рішенням РНБО від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України", затвердженим Указом Президента України від 01.05.14 р. № 449/2014 [15]. Згідно з цим рішенням Кабінету Міністрів України було доручено розробити й подати на розгляд парламенту законопроекти про внесення змін у закони України щодо протидії інформаційній агресії іноземних держав, передбачивши, зокрема:

визначення механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів; запровадження для іноземних ЗМІ системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп. Крім того, приписувалося підготувати проект стратегії розвитку інформаційного простору України, розробити і впровадити комплексні заходи організаційного, інформаційного й роз'яснювального характеру щодо всебічного висвітлення заходів з реалізації державної політики у сфері забезпечення інформаційної безпеки, а також посилити контроль за дотриманням законодавства з питань інформаційно-психологічної та кібернетичної безпеки. Відповідно до вказаного плану заходів й було розроблено Доктрину інформаційної безпеки України [14].

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу РФ в умовах розв'язаної нею гібридної війни. Її правовою основою є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента від 26 травня 2015 року № 287, а також міжнародні договори, згода на обов'язковість яких надана Верховною Радою України.

У тексті Доктрини йдеться про національні інтереси України в інформаційній сфері, актуальні загрози національним інтересам та національній безпеці, пріоритети державної політики в інформаційній сфері й механізм її реалізації. Втілення положень цього документа покладено на Кабінет Міністрів, Міністерство інформаційної політики, Міністерство закордонних справ, Міністерство культури України, Державне агентство України з питань кіно, Національну раду України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України, Службу безпеки України, розвідувальні органи, Державну службу спеціального зв'язку та захисту інформації, Національний інститут стратегічних досліджень, а також на Верховну Раду України, оскільки Доктриною передбачається внесення змін до чинного законодавства України.

Доктрина спрямована на захист українського суспільства від "агресивного інформаційного впливу Російської Федерації", розвиток публічної дипломатії, в тому числі культурної та цифрової, видалення шкідливої інформації з українського сегменту Інтернету та квотування національного аудіовізуального контенту, захист права на вільний доступ до інформації, створення механізмів захисту від пропаганди тощо.

Утім, в експертному середовищі Доктрина отримала переважно негативну оцінку, на кшталт: "Доктрина інформаційної безпеки України – це лише декларація" або "Замість інтеграції Україна встановлює паркан" тощо. Справді, у Доктрині держава виклала бачення розвитку й функціонування свого інформаційного простору і визначила, що Російська Федерація є противником, котрий веде системну інформаційну війну. У документі є пропозиції, як реагувати на агресію та забезпечувати інформацією громадян. Доктрина також визначає поняття "стратегічного наративу" і вказує, що медіа мають самі себе регулювати, але при цьому мають нести соціальну відповідальність. Доктрина закладає державну систему постійного моніторингу веб-ресурсів та блокування сайтів, що загрожують безпеці, однак виписані в документі підстави для блокування доволі абстрактні – орган державної влади на свій розсуд зможе тлумачити, що загрожує безпеці, а що ні. Відповідно, виникає небезпека встановлення цензурних шлюзів, які відокремлять український Інтернет від світу. Крім того, механізм реалізації Доктрини, навіть у її позитивних аспектах, не містить жодної конкретики, тож у чинній редакції вона не може слугувати базовим документом, на підставі якого мають формуватися й інші правові акти у сфері забезпечення інформаційної безпеки, в тому числі стратегічні та програмні.

Відтак, сьогодні вкотре слід порушувати питання щодо розробки нормативного акта (закону), яким визначатиметься єдиний поняттєво-категорійний апарат, державна політика забезпечення інформаційної безпеки, об'єкти інформаційної безпеки та суб'єкти її забезпечення, правові зони відповідальності відомств, залучених до сфери забезпечення інформаційної безпеки, механізми координування їх діяльності щодо реагування на виклики та загрози національній безпеці в інформаційній сфері, порядок правового закріплення взаємовідносин державних безпекових структур з іншими органами та відомствами, віднесеними законодавством до суб'єктів забезпечення національної безпеки України, тощо [16, с. 37-38]. Вважаємо, що такий нормативний акт неодмінно має дати чітке визначення як системи інформаційної безпеки, так і системи забезпечення інформаційної безпеки.

Усе це зайвий раз доводить нагальну потребу розробки та прийняття Закону України "Про інформаційну безпеку України" як базового нормативно-правового акта, що регулюватиме відповідні питання [17, с. 89]. Такий закон як фундамент для побудови ефективної стратегії інформаційної безпеки має містити не абстрактні декларації, а чітко визначені основоположні категорії у сфері інформаційної безпеки та підходи до формування системи її забезпечення, механізм її функціонування, повноваження і схему взаємодії суб'єктів забезпечення інформаційної безпеки тощо.

Дане зумовлюється і досить динамічним розвитком інформаційного суспільства. У цьому ракурсі ми поділяємо думку В. Брижка, що у наш час життєдіяльність світової цивілізації дедалі більше спрямовується інформаційною сферою, яка завдяки інформаційно-технологічним змінам, що почалися наприкінці XX століття, об'єктивно зумовили появу нового типа суспільства – інформаційного суспільства [19, с. 20]. Досить цікавою у ракурсі даного дослідження є думка В. Фурашева про те, що інформаційний простір – це форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі [20, с. 166].

Висновки.

Сьогодні Україна відстоює свій євроінтеграційний курс в умовах окупації Криму й частини Донецької та Луганської областей унаслідок неоголошеної війни, яка ведеться Російською Федерацією проти нашої держави з активним використанням методів інформаційного протиборства. У зв'язку зі значним негативним інформаційним впливом на інформаційний суверенітет нашої держави, питання правового забезпечення кібербезпеки України набувають особливої актуальності.

Можливо багато говорити про важливість і актуальність посилення регулювання на національному та міжнародному рівнях діяльності в кіберпросторі і зростання ролі в цьому і приватного сектора; встановлення контролю над кіберзброєю, а також посилення охорони критичної інфраструктури України; впровадження інновацій в сфері кібербезпеки та вдосконалення освітніх напрямів підготовки фахівців даної сфери діяльності тощо. Однак без набуття системного та комплексного характеру всі зазначені підходи не дозволять вивести рівень кібербезпеки, а звідси – і національної безпеки України загалом, на новий якісний рівень. Боротьба з кіберзлочинністю повинна носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Ефективність заходів у цій сфері повинна досягатися завдяки здійсненню оцінки загроз організованої кіберзлочинності, що дозволить визначати сучасні загрози та ризики у кіберпросторі.

Використана література

1. Присяжнюк М.М. Інформаційна безпека України в сучасних умовах. *Вісник Київського національного університету імені Тараса Шевченка. Військово-спеціальні науки*. 2013. Вип. 30. С. 42-46.

2. Конституція України: Основний Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon3.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 05.12.2019).

3. Цимбалюк В. Окремі питання щодо визначення категорії "інформаційна безпека" у нормативно-правовому аспекті. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник*. Київ, 2004. С. 30-33.

4. Рубан В.Я. Інформаційна безпека України: сутність та проблеми. Стратегічна панорама. 1998. № 3-4. С. 170-175.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. URL: http://zakon3.rada.gov.ua/laws/show/2163-19 (дата звернення 05.12.2019).

6. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір: монографія. Київ: ТОВ "Видавничий дім "АртЕк", 2018. 422 с.

7. Европейская Конвенция по киберпреступлениям. URL: http://inter.criminology.onua.edu.ua/?p=2263 (дата звернення: 05.12.2019)

8. Брижко В.М. та ін. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. – (НДЦПІ АПрН України). Київ: Видавництво ТОВ "Пан-Тот", 2007 р. 234 с.

9. Окінавська хартія глобального інформаційного суспільства від 22.07.2000 р. URL: http://zakon4.rada.gov.ua/laws/show/998_163 (дата звернення 05.12.2019).

10. Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada URL: http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf (дата звернення 05.12.2019).

11. The Department Of Defense Cyber Strategy URL: http://www.defense.gov/home/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата звернення 05.12.2019).

12. Ткачук Т.Ю. Механізми протидії інформаційним загрозам зовнішніх джерел. *Вісник НТУ України "Київський політехнічний інститут". Політологія. Соціологія. Право*. 2017. № 1–2. С. 242-246.

13. Ткачук Т.Ю. Кібербезпека: підходи до визначення в окремих країнах: мат. наук.-практ. конф. *Актуальні проблеми управління інформаційної безпекою держави,* м. Київ, 24.05.17 р. Київ: Нац. акад. СБУ, 2017. С. 142-144.

14. 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: www.president.gov.ua/documents/472017-21374 (дата звернення 05.12.2019).

15. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України": Указ Президента України від 01.05.14 р. № 449/2014. URL: www.president.gov.ua/documents/4492014-17157 (дата звернення 05.12.2019).

16. Довгань О.Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: матеріали круглого столу *Філософсько-правові та прикладні аспекти*, м. Вінниця 12 травня 2017 р., Вінницький державний педагогічний університет ім. М. Коцюбинського / упоряд.: О.Д. Довгань, М.В. Беланюк, С.А. Лапшин, О.Г. Радзієвська, О.І. Яременко [та ін.]. Київ: Видавничий дім "АртЕк", 2017. С. 31-39.

17. Довгань О.Д. Ткачук Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України. *Інформація і право*. 2019. № 1. С. 86-100.

18. Довгань О.Д., Доронін І.М. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту: монографія. – (НДІІП НАПрН України). Київ: Видавничий дім "АртЕк". 2017. 107 с.

19. Брижко В.М. Філософія права: герменевтика в сфері інформаційного права. *Правова інформатика*. № 1(41)/2014. С. 18-22.

20. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. № 2(5)/2012. С. 162-169.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.351/354

КОРЖ І.Ф., *доктор юридичних наук, старший науковий співробітник*,
завідувач наукової лабораторії НДІ інформатики і права НАПрН України

ПРАВОВА БЕЗПЕКА СФЕРИ ДОСТУПУ ГРОМАДЯН ДО УПРАВЛІННЯ ДЕРЖАВНИМИ СПРАВАМИ

Анотація. *В даній статті досліджується питання стану правової безпеки сфери доступу громадян до управління державними справами; аналізується стан правового забезпечення реалізації зазначеного конституційного права нормами матеріального і процесуального права. Розкрито національні та міжнародно-правові механізми забезпечення реалізації зазначеного права; наводяться недоліки у реалізації політичного права на участь громадян в управлінні державними справами.*

Ключові слова: *громадські ради; конституційне право; міжнародно-правові стандарти; політичне право; правова безпека; управління державними справами.*

Summary. *This article analyzes the state of legal security in the sphere of citizens' access to the management of state affairs; analyzes the state of legal support for the implementation of this constitutional right by substantive and procedural law. National and international legal mechanisms for ensuring the implementation of this right are disclosed; deficiencies in the implementation of the political right of citizen to participate in the management of state affairs are considered.*

Keywords: *public councils; constitutional law; international legal standards; political law; legal security; management of state affairs.*

Аннотация. *В данной статье исследуется вопрос состояния правовой безопасности сферы доступа граждан к управлению государственными делами; анализируется состояние правового обеспечения реализации указанного конституционного права нормами материального и процессуального права. Раскрыты национальные и международно-правовые механизмы обеспечения реализации указанного права; рассматриваются недостатки в реализации политического права на участие граждан в управлении государственными делами.*

Ключевые слова: *общественные советы; конституционное право; международно-правовые стандарты; политическое право; правовая безопасность; управления государственными делами.*

Постановка проблеми. Відповідно до положень статті 38 Конституції України громадяни мають право брати участь в управлінні державними справами, що відповідає міжнародним нормам.

Питанням права громадян на участь в управлінні державними справами 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 комплексний характер дослідження цього права, особливості його реалізації вимагають продовження наукових досліджень і, насамперед, в частині правового регулювання його реалізації, розглядаючи зазначене через призму "правової безпеки" сфери доступу громадян до управління державними справами.

Метою статті є визначення засад правового регулювання доступу громадян до управління державними справами та встановлення його стану, виділення проблемних питань, які потребують нагального розв'язання, а також розкриття поняття "правова безпека" сфери доступу громадян до управління державними справами.

Виклад основного матеріалу. Необхідно зазначити, що розвинуте демократичне та громадянське суспільство можна побудувати лише в державі, де громадяни є активними учасниками процесу формування та реалізації державної політики. З цією метою публічною владою розробляються та здійснюються заходи, що сприятимуть становленню громадянського суспільства, підвищуватимуть рівень правової культури громадян, створюватимуть умови для ширшої обізнаності громадян під час проведення діалогу з владою [1].

Визначальною рисою сучасного розвитку держав у світі є заохочення громадян та їх об'єднань до активної участі у розвитку концепції прав людини і основоположних свобод в їх захисті, використовуючи такі засоби, як національне і міжнародне право, оскільки права людини стають глобальним мірилом права [2, с. 375]. Міжнародними стандартами в галузі прав людини і громадянина є загальновизнані принципи і норми міжнародного права, втілені у міжнародно-правових документах (у міжнародних договорах, документах недоговірного характеру, у рішеннях міжнародних судів, зокрема Європейського суду з прав людини), до забезпечення яких прагне будь-яка цивілізована держава як член світового співтовариства. Тому міжнародно-правовими стандартами демократії є закріплені у міжнародному праві юридичні зобов'язання, авторитетно підтримувані орієнтири соціального і політичного розвитку [3, с. 13].

Основними документами, у яких знайшли втілення універсальні міжнародно-правові стандарти участі громадян в управлінні державними справами у політичній сфері, є:

– Загальна декларація прав людини 1948 р. [4];

– Міжнародний пакт про громадянські й політичні права 1966 р. (підписаний УРСР 20.03.1968 р.; ратифікований 19.10.1973 р.; набув чинності для України 23.03.1976 р.) [5].

Відповідно до частини 1 ст. 21 Загальної декларації прав людини, "кожна людина має право брати участь в управлінні своєю державою безпосередньо чи за посередництвом вільно обраних представників". Це положення розвивається у частині 2 ст. 21: "кожна людина має право рівного доступу до державної служби у своїй країні"; частина 3: "воля народу повинна бути основою влади уряду; ця воля повинна знаходити вираження в періодичних і нефальсифікованих виборах, що мають проводитися при загальному і рівному виборчому праві, шляхом таємного голосування або ж за допомогою інших рівнозначних форм, що забезпечують свободу голосування" [4].

На положеннях Загальної декларації прав людини ґрунтується обов'язковий для держав Міжнародний пакт про громадянські й політичні права. Відповідно до ст. 25 Пакту, "кожен громадянин повинен мати без дискримінації і без необґрунтованих обмежень право і можливість: а) брати участь у веденні державних справ як безпосередньо, так і за посередництвом вільно обраних представників; б) голосувати і бути обраним на справжніх періодичних виборах, що проводяться на основі загального і рівного виборчого права при таємному голосуванні і забезпечують вільне волевиявлення виборців; в) допускатися у своїй країні на загальних умовах рівності до державної служби" [5].

Окрім розглянутих вище основоположних актів з прав людини, що були прийняті на рівні ООН, в рамках цієї організації розроблені інші специфічні документи стосовно основних демократичних політичних цінностей. Так, у Резолюції 53/31 Генеральної Асамблеї ООН "Підтримка системою Організації Об'єднаних Націй зусиль урядів з розвитку і зміцнення нових чи відроджених демократій" від 23 листопада 1998 р. вказано, що демократія ґрунтується на вільному волевиявленні народу, що дозволяє

йому визначати свою власну політичну, економічну, соціальну і культурну систему, і на його всебічній участі у всіх аспектах його життя [6].

Такими є акти Ради Європи, як то Європейська конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. (підписана Україною 09.12.1995 р.; ратифікована Україною 17.07.1996 р. [7] з протоколами, у яких доповнені чи уточнені окремі її положення; документи Організації з безпеки та співробітництва в Європі – Європейська соціальна хартія від 18 жовтня 1961 року [8]. Європейська конвенція гарантує головним чином громадянські та політичні права (на зразок Міжнародного пакту про громадянські та політичні права), тобто права першого покоління.

Засади громадянської участі в управлінні закладені також в Резолюціях та інших актах Парламентської Асамблеї Ради Європи (далі – ПАРЄ). Так, у Резолюції 980 (1992) "Про участь громадян у політиці" [9] ПАРЄ підтверджує: "демократія атрофується без широкої участі громадян, з якими повинні, де це можливо, консультуватися з питань, що їх безпосередньо стосуються, за допомогою відповідних механізмів" (п. 2). На виконання цієї Резолюції була прийнята Рекомендація ПАРЄ 1180 (1992) "Про участь громадян у політиці" [10], яка наголошує на важливій ролі неурядових організацій (асоціацій, фондів, рухів або груп, незалежних від уряду, заснованих на некомерційній основі для захисту певних інтересів) у розвитку участі громадян у політичному житті. Інші акти, такі як Резолюція ПАРЄ 1121 (1997) "Про інструменти участі громадян у представницькій демократії" та Резолюція ПАРЄ 1154 (1998) "Демократичне функціонування національних парламентів" наголошують, що дієвість демократії залежить від активного внеску всіх громадян. Їх участь у політичному житті та співробітництво в межах політичних інституцій є вирішальним фактором налагодженого функціонування демократичних інституцій (установ*)*. Тому ПАРЄ звернула увагу на необхідність більш широкої участі громадян у прийнятті політичних рішень.

Відповідно до підсумкового Документа Копенгагенської наради Конференції з людського виміру ОБСЄ (1990 р.) [11], держави-учасниці поважають право своїх громадян брати участь в управлінні державою безпосередньо або через представників, що обираються ними вільно у ході чесного виборчого процесу (п. 6); право громадян добиватися політичних чи державних посад в особистій якості або як представників політичних партій чи організацій без дискримінації (7.5); право створювати в умовах повної свободи політичні партії чи інші політичні організації, яким надаються необхідні юридичні гарантії, що дозволяють їм змагатися одна з одною на основі рівності перед законом і органами влади (7.6). Закон і державна політика мають допускати проведення політичних кампаній в атмосфері свободи і чесності, у якій жодні адміністративні дії, насильство і залякування не утримували б партії і кандидатів від вільного викладу своїх поглядів і оцінок, а також не заважали б виборцям голосувати вільно, не побоюючись покарання (7.7).

Закріплення політичних прав і свобод громадян України на конституційному рівні є важливою гарантією їх здійснення. Але воно ще не забезпечує дотримання, використання і захист цих прав у реальному політико-правовому житті. Тому необхідним є дослідження і вдосконалення всіх конституційно-правових гарантій та механізму реалізації права участі громадян в управлінні державними справами, за відсутності яких усілякі права і свободи людини залишаються в теорії. Для практичної реалізації будь-якого суб'єктивного права важливо не тільки записати й урочисто проголосити норму про відповідне право в Конституції, але й докласти зусиль для того, щоб люди її засвоїли, щоб її виконання підкріплювалося системою реальних конституційно-правових гарантій, напрацювання відповідного законодавчого механізму їх реалізації та забезпечення.

Таким чином, відсутність чи неналежне забезпечення законодавчого врегулювання певних процедурних питань щодо здійснення громадянами їх конституційних політичних прав і свобод іноді призводить до того, що людина не може вирішити питання, які виникли у процесі їх реалізації. Саме чинне законодавство має утворювати ефективні механізми і гарантії їх реалізації. Тому права громадян, щодо їхньої участі в управлінні державними справами, конкретизуються й деталізуються в законодавстві – у законах України "Про громадські об'єднання", "Про політичні партії в Україні", "Про всеукраїнський референдум", "Про державну службу", "Про звернення громадян" тощо.

Органи держави мають організаційно забезпечувати можливість здійснення права громадян України на участь в управлінні шляхом нормотворення, правозастосування, правоохоронної (правозахисної) діяльності. В організаційному забезпеченні реалізації цього права визначальною є діяльність не тільки державних органів і посадових осіб, але й органів місцевого самоврядування, політичних партій та громадських організацій. Одним із таких механізмів забезпечення зазначеного є Постанова Уряду [12]. Постановою затверджено Порядок проведення консультацій з громадськістю з питань формування та реалізації державної політики та Типове положення про громадську раду при міністерстві, іншому центральному органі виконавчої влади, Раді міністрів Автономної Республіки Крим, обласній, Київській та Севастопольській міській, районній у м. Києві та Севастополі державній адміністрації. Крім того, рекомендовано органам місцевого самоврядування під час проведення консультацій з громадськістю та утворення громадських рад при органах місцевого самоврядування керуватися затвердженими цією постановою Порядком і Типовим положенням.

Порядок визначає основні вимоги до організації і проведення органами виконавчої влади консультацій з громадськістю з питань формування та реалізації державної політики. Консультації з громадськістю проводяться з метою залучення громадян до участі в управлінні державними справами, надання можливості для їх вільного доступу до інформації про діяльність органів виконавчої влади, а також забезпечення гласності, відкритості та прозорості діяльності зазначених органів. Проведення консультацій з громадськістю має сприяти налагодженню системного діалогу органів виконавчої влади з громадськістю, підвищенню якості підготовки рішень з важливих питань державного і суспільного життя з урахуванням громадської думки, створенню умов для участі громадян у розробленні проектів таких рішень.

Відповідно до Типового положення, основним завданням громадської ради є сприяння реалізації громадянами конституційного права на участь в управлінні державними справами та забезпечення врахування громадської думки у процесі підготовки та організації виконання рішень центральних і місцевих органів виконавчої влади. До складу громадської ради включаються представники громадських організацій, професійних спілок та інших об'єднань громадян, органів місцевого самоврядування, засобів масової інформації.

Таким чином, реалізація права громадян України брати участь в управлінні державними справами – це процес (а зрештою, і результат) втілення конституційно-правових норм про зазначене право у практичну діяльність. Її ефективність багато в чому залежить від чіткого конституційного механізму реалізації таких норм в діяльності суб'єктів державно-правових відносин. Політичне і практичне значення реалізації цього права полягає в тому, що саме в реалізації це стрижневе політичне право набуває реальності, а отже, й дійсної соціально-політичної цінності.

Поряд з такими формами участі в управлінні державними справами громадян як, участь у реалізації правосуддя, у виборах різного рівня депутатів, референдумах,

мітингах тощо, відносно новою такою формою є електронна петиція, як різновид звернення громадян до органів державної влади, місцевого самоврядування, об'єднань громадян, підприємств, установ, організацій незалежно від форм власності, засобів масової інформації, посадових осіб відповідно до їх функціональних обов'язків із зауваженнями, скаргами та пропозиціями, що стосуються їх статутної діяльності, заявою або клопотанням щодо реалізації своїх соціально-економічних, політичних та особистих прав і законних інтересів та скаргою про їх порушення [13].

Ураховуючи підвищення ролі громадянського суспільства в різних сферах діяльності органів державної влади та органів місцевого самоврядування, зокрема щодо впровадження реформ, на підтримку ініціативи громадськості, а також з метою налагодження ефективного діалогу та партнерських відносин органів державної влади, органів місцевого самоврядування з організаціями громадянського суспільства, передусім з питань забезпечення прав і свобод людини і громадянина, Президентом України був прийнятий відповідний Указ [14], яким затверджена Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2016 – 2020 роки, що зумовлено необхідністю створення державою сприятливих умов для розвитку громадянського суспільства, різноманітних форм демократії участі, налагодження ефективної взаємодії громадськості з органами державної влади та органами місцевого самоврядування.

Прикладом нових форм політичної участі громадян є залучення не тільки до формування вищих органів державної влади (вибори), але й до розробки законопроектів, вироблення і реалізації проектів державних політичних рішень (громадські експертні консультативні ради при вищих державних органах; громадські обговорення законопроектів та інших рішень); громадський контроль – наприклад, система регулярних зустрічей і звітів не тільки народних депутатів, але й посадових осіб органів управління перед громадянами; участь у роботі політичних партій, відповідних громадських організацій (наприклад, Комітету виборців України), участь у політичних кампаніях, проведенні правових освітніх і виховних заходів тощо. Тобто існує різноманітність, гнучкість, відповідна зручність форм участі громадян в управлінні.

Таким чином можна стверджувати, що в Україні створена і функціонує система забезпечення участі громадян в управлінні державними справами в індивідуальній та колективній формах. Для зазначеного напрацьована відповідна правова база, що дає змогу говорити про забезпечення належного правового регулювання в зазначеній сфері. Тим самим, можна говорити про забезпечення правової безпеки сфери участі громадян в управлінні державними справами.

Однак, поряд із зазначеним постає питання щодо ефективності механізму забезпечення згаданого права, а це вказує на існування певних процесуальних проблем щодо забезпечення належної правової безпеки цієї сфери. Саме у проблемі щодо практичної (процесуальної) реалізації матеріальних норм права і постає загроза правовій безпеці України, оскільки існуючі процесуальні норми не гарантують дієвої участі громадян в забезпеченні їхньої участі в управлінні державними справами.

Так, для сприяння участі громадян у процесах прийняття державних рішень, перепоною залишається існування в Україні таких умов, за яких існуючий в Україні рівень корупції (за результатами 2018 року, Україна має 32 бали зі 100 максимально можливих, і у рейтингу "Індекс сприйняття корупції" займає 120-е місце серед 180 країн) [15] не дає змоги громадянському суспільству функціонувати та вільно й активно брати участь у процесах прийняття рішень, включно й тих, що стосуються розробки політики та законів.

Наступною проблемою є питання неналежного дотримання в Україні верховенства права та реалізації інших прав людини та основоположних свобод, включно із економічними правами, а саме повноцінного та рівноправного гарантування права на доступ до інформації тощо. 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].

Проблемою також є слабка політична воля, що сприяє участі об'єднань громадян у процесах прийняття державних рішень, а також заохочує, підтримує та цінує вклад громадянського суспільства. Прикладом зазначеного можуть слугувати дії екс-міністра соціальної політики Реви А.О. щодо ігнорування можливості дієвої участі, врахування думок, пропозицій до законодавства ветеранських і громадських організацій у процесі проведення пенсійної реформи у воєнній сфері. Зазначене вилилось у жорстке протистояння представників громадянського суспільства і державної влади та несприйняття ухвалених новел в пенсійному законодавстві, а також до підвищення соціальної напруги в громадському середовищі.

Наступна проблема – у значній кількості залишається негативне ставлення державних органів влади до включення у риторику обговорень чи діалогу критики та відмінних точок зору з боку громадянського суспільства. Зазначене вказує на недостатню культуру діалогу між тими, хто приймає рішення (органами публічної влади) та громадянським суспільством, яка має сприяти зміцненню взаємодовіри. Тому лише здатність як державних установ (уряду), так і об'єднань громадян залучатися до змістовних дискусій, за умови, що відсутність такої можливості не становить перешкоди або не використовується як виправдання відмови об'єднанням громадян в участі в процесах прийняття рішень.

Актуальним ще залишається побудова в Україні вільного, незалежного та активного громадянського суспільства, що має змогу розвиватися та рости, особливо завдяки наданню та доступу до ресурсів (фінансових, людських та технологічних), включно з доступом до міжнародного фінансування. Відповідно до міжнародних актів, громадським об'єднанням має надаватися можливість брати участь у процесах прийняття рішень на усіх рівнях (місцевому, національному, регіональному та міжнародному), а також на усіх етапах цих процесів, починаючи з планування та розробки політики, до моменту реалізації рішень, їх моніторингу та оцінки. Усі об'єднання громадян та окремі громадяни повинні мати дієвий доступ до правосуддя, регіональних та міжнародних механізмів захисту прав людини, а також мати змогу вільно використовувати та комунікувати через ці механізми, не боячись за це настання черех це юридичних наслідків.

Міжнародні організації рекомендують при вирішенні зазначених проблем опиратися на наступні міжнародні документи, такі як:

– Конвенція Європейської Економічної Комісії ООН про доступ до інформації, участь громадськості у процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля (Оргуська конвенція) від 25 червня 1998 року;

– Декларації ООН про правозахисників від 8 березня 1999 року та Резолюція Ради ООН з прав людини щодо захисту правозахисників від 21 березня 2013 року;

– Резолюція Ради ООН з прав людини “Простір громадянського суспільства: створення та підтримка безпечних та сприятливих умов на законодавчому рівні та на практиці” від 23 вересня 2013 року;

– Конвенція Ради Європи щодо доступу до офіційних документів від 18 червня 2009 року (CETS № 205);

– Рекомендація Ради Європи CM/Rec (2007) 14 щодо юридичного статусу неурядових організацій у Європі;

– Кодекс Ради Європи кращих практик участі громадськості у процесі прийняття рішень (2009 року);

– Керівні принципи щодо підтримки ЄС громадянського суспільства у країнах “розширення ЄС” (2014 – 2020).

Як показує практика, навіть за наявності необхідних процесуальних норм, і водночас, за відсутності відповідної політичної волі з боку державної влади, гарантувати забезпечення належного функціонування матеріальних правових норм не можна. Тим самим актуалізується питання щодо необхідності забезпечення належного стану правової безпеки в даній сфері. З огляду на зазначене правовій безпеці сфери участі громадян в управлінні державними справами можна дати наступне визначення: це стан законодавчого регулювання дієвої участі громадян в управлінні державними справами, за якого суспільство спроможне належно та ефективно вирішувати питання, пов’язані з функціонуванням та розвитком людини, суспільства та держави.

Висновки.

Підсумовуючи викладене вище, доцільно зазначити, що участь громадян в управлінні державними справами не є даниною сучасній “політичній моді” – це вимога нинішнього часу і потреба майбутнього будь-якого суспільства. Україна йде в ногу із зазначеними вимогами і потребами, напрацьовуючи відповідне правове підґрунтя для реалізації та забезпечення зазначеного – напрацьовані відповідні національні правові засади, які базуються на міжнародно-правових актах. Тим самим можна стверджувати про забезпечення відповідного рівня правової безпеки сфери участі громадян в управлінні державними справами. Однак, зазначені у дослідженні недоліки вказують на наявні проблеми у забезпеченні зазначеного конституційного і політичного права громадян України, і значною мірою воно залежить від прояву відповідної політичної волі влади. А це, у свою чергу, вказує на наявні проблеми правової безпеки держави в цілому і на актуальність вирішення згаданих проблем.

Використана література

1. Злобін С.В. та ін. Наші права: участь громадян в управлінні державними справами; за заг. ред. Н.К. Дніпренка. Вінниця: ТОВ “Консоль”, 2006. 64 с.

2. Адміністративне право України: підручник для юрид. вузів і фак.; за ред. Ю.П. Битяка. Харків: Право, 2000. 520 с.

3. Авер`янов В.Б. Державний апарат. Юридична енциклопедія: у 6 т. Київ: Укр. енцикл., 1998. Т. 2. 1999. 741с.

4. Загальна декларація прав людини прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. *Офіційний вісник України*. 2008. № 93. С. 89.

5. Міжнародний пакт про громадянські й політичні права від 16 грудня 1966 р. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення 30.08.2019).

6. Підтримка системою Організації Об’єднаних Націй зусиль урядів з розвитку і зміцнення нових чи відроджених демократій: Резолюція 53/31 Генеральної Асамблеї ООН від 23 листопада 1998 р. URL: https://zakon.rada.gov.ua/rada/show/995_610/sp:max100 (дата звернення 30.08.2019).

7. Про захист прав людини і основоположних свобод: Європейська конвенція від 04 листопада 1950 р. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення 05.09.2019).

8. Європейська соціальна хартія від 18 жовтня 1961 р. URL: https://zakon.rada.gov.ua/laws/show/994_300 (дата звернення 05.09.2019).

9. Parliamentary Assembly of the Council of Europe. Resolution 980 (1992) on citizens' participation in politics. Text adopted by the Assembly on 7 February 1992 (26th Sitting) URL: http://assembly.coe.int/Documents/AdoptedText/ta92/ ERES980. htm (дата звернення 05.09.2019).

10. Parliamentary Assembly of the Council of Europe. Recommendation 1180 (1992) on citizens' participation in politics. Text adopted by the Assembly on 7 February 1992 (26th Sitting) URL: http://assembly.coe.int/Documents/Adopted Text/ta92/EREC1180.htm (дата звернення 05.09.2019).

11. Документ Копенгагенської наради Конференції з людського виміру ОБСЄ від 29 червня 1990 р. URL: https://zakon.rada.gov.ua/laws/show/994_082 (дата звернення: 05.09.2019).

12. Про забезпечення участі громадськості у формуванні та реалізації державної політики: Постанова Кабінету Міністрів України від 03.11.10 р. № 996. *Офіційний вісник України*. 2010. № 84. С. 36.

13. Про звернення громадян: Закон України від 02.10.96 р. № 393/96-ВР. *Відомості Верховної Ради України.* 1996. № 47. Ст. 256.

14. Про сприяння розвитку громадянського суспільства в Україні: Указ Президента України від 26.02.16 р. № 68/2016. *Офіційний вісник Президента України*. 2016. № 7. С. 32.

15. CPI-2018: Україна знову гірше всіх сусідів, окрім Росії. URL: https://ti-ukraine.org/news/cpi-2018-ukrayina-znovu-girshe-vsih-okrim-rosiyi/?fbclid=IwAR0MV41PbYANN-USga7BbEFO_c4QbU4frX_YBCI26vYQb3gChAG-Sn9M0vI (дата звернення 15.09.2019).

16. Березовська І. Актуальні питання доступу громадян до публічної інформації та проблеми застосування Закону України "Про доступ до публічної інформації". URL: http://ena.lp.edu.ua:8080/bitstream/ntb/37396/1/5_26-31.pdf (дата звернення 15.09.2019).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.3(308)

ЗОЛОТАР О.О., *доктор юридичних наук, старший науковий співробітник,*
завідувач науковим сектором НДІ інформатики і права НАПрН України

СОЦІОЛОГІЧНІ ДОСЛІДЖЕННЯ У ВИБОРЧОМУ ПРОЦЕСІ ЯК ЧИННИК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Анотація. *Досліджується вплив результатів соціологічних досліджень на формування суспільної думки у виборчому процесі.*

Ключові слова*: соціологічні дослідження, виборчий процес, демократія, інформаційний вплив.*

Summary*. The influence of the sociological research results on the formation of public opinion in the electoral process is investigated.*

Keywords*: sociological research, electoral process, democracy, information influence.*

Аннотация*. Исследуется влияние результатов социологических исследований на формирование общественного мнения в избирательном процессе.*

Ключевые слова*: социологические исследования, избирательный процесс, демократия, информационное воздействие.*

Постановка проблеми. Виборчий процес як діяльність з формування керівних органів влади у державі залишається однією з найбільш поширених форм демократії. Поруч з реалізацією національного і народного суверенітету та легітимізацією влади важливою функцією виборів є формування і вираження суспільної думки. У сучасному виборчому процесі щораз значимішою є роль соціологічних досліджень у виборчих кампаніях, при тому їх вплив на виборчий процес в цілому і на виборців, зокрема, не має однозначної оцінки з боку науковців – соціологів, юристів і політологів.

Водночас, наявність соціологічних досліджень та рівень їх впливу на суспільну думку свідчить про демократичність суспільства. В авторитарних закритих суспільствах стан справ не підлягає соціологічному вивченню, а тим більше публічному обговоренню і громадському контролю [1, с. 9].

У широкому розумінні до змісту поняття “електоральної поведінки” включають не лише сам акт делегування повноважень (на етапі голосування), але й процес прийняття рішень та соціальні фактори, що впливають на модель голосування. Широке використання у виборчих кампаніях результатів соціологічних досліджень не лише для безпосереднього вивчення ідеологічних, політичних уподобань електорату та прогнозування результатів голосування, але й з прихованою метою формування та «регулювання» громадської думки, потребує нових досліджень чинників електоральної поведінки та технологій впливу на виборців [2, с. 41].

Результати соціологічних досліджень, зокрема, рейтинги політичних сил та окремих кандидатів, використовуються не лише як соціологічна інформація, а як інформаційна зброя. ЗМІ публікує ці дані з посиланням на невідомі або маловідомі центри без обов’язкової методологічної інформації для оцінки якості даних. Іноді серйозні видання та провідні телевізійні канали публікують дані опитування 20 тисяч респондентів, проведених за 1 день центрами, які не описують спосіб відбору респондентів та метод збору даних. Маловідомі або зовсім не відомі організації проводять прес-конференції, на яких презентують результати псевдоопитувань. Все це призводить

до інфляції цінності професійної соціологічної інформації і не дає можливості суспільству відокремити реальні виміри громадської думки від їхньої імітації [3].

Елвін Тоффлер в його "Метаморфозах влади" [4] ще в 1990 році писав: "Інформаційні війни вирують в наших душах, адже йдеться про те, як люди думають, як приймають рішення та яку використовують систему знань і уявлень. Уява при цьому є настільки ж важливим чинником, як і інформація взагалі".

Дослідження є актуальним і з огляду на вибори Президента України та вибори до Верховної Ради України, що відбулись в 2019 році. Адже передвиборча агітація і особливості інформаційного забезпечення цих виборів надали розгорнутий емпіричний матеріал для цього дослідження.

Результати аналізу наукових публікацій. Досліджуване питання знаходиться на межі кількох наукових напрямів – соціології (зокрема, соціології права), науки про безпеку, політології, а також інформаційного та конституційного права. Одними із перших, хто звернув увагу на інформаційні впливи при реалізації демократії були соціологи-футурологи Е. Тоффлер [4] і М. Мак-Люєн [5]. Електоральна соціологія є відносно новим напрямком для української соціологічної науки.

Комплексні правові дослідження цього питання на сьогодні відсутні. Окремі аспекти досліджувались в працях Брижка В. [6], Богдан О. [1], Довганя О. [7], Додонова Д. [8], Жванія Т. [2], Почепцова Г. [9], Поліщук І. [10], Фурашева В. [11] та інших.

Водночас, стан правового регулювання соціологічних досліджень під час виборчого процесу, а також їх вплив на інформаційну безпеку людини, держави і суспільства потребує наукового опрацювання.

Метою статті є соціолого-правовий аналіз оприлюднення результатів досліджень громадської думки у виборчому процесі в контексті інформаційної безпеки.

Виклад основних положень.

Правове регулювання досліджень громадської думки та оприлюднення їх результатів.

Аналіз норм Закону України "Про інформацію" [12] дозволяє віднести результати дослідження громадської думки до соціологічної інформації, оскільки ст. 19 чинної редакції цього Закону визначає, що "соціологічна інформація – це будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо". Цією ж статтею передбачено, що правовий режим такої визначається законами та міжнародними договорами України, згода на обов'язковість яких надана Верховною Радою України.

З такого визначення "соціологічної інформації" можна зробити висновки, що для того щоб відомості стали соціологічною інформацією достатньо, щоб вони були задокументовані і відображали ставлення до окремих осіб, подій, явищ, процесів, фактів тощо. Це дозволяє також зробити висновок про легітимність кожного джерела соціологічної інформації, і свободу вибору методології та методики досліджень. І з цього також слідує, що кожен суб'єкт інформаційних відносин має право бути джерелом соціологічної інформації, а до таких відповідно до ст. 4 згаданого Закону належать фізичні особи та юридичні особи, об'єднання громадян, а також суб'єкти владних повноважень.

В редакції згаданого Закону, що існувала до 9 травня 2012 року, було закріплено також основні джерела соціологічної інформації і хто саме здійснює соціологічні дослідження – "державні органи і об'єднання громадян, зареєстровані у встановленому порядку". Проте зараз цієї норми немає. Відповідно здійснювати соціологічні дослідження може хто завгодно і без обов'язку жодної реєстрації.

Наслідком такої законодавчої неврегульованості є ситуація, що склалась. Поруч із фаховими і професійними соціологічними дослідженнями, що здійснюються інституціями різних форм власності, проте які цінують власну репутацію, з'являються передвиборчі "метелики-одноденки" – організації, які часто не є навіть юридичними особами, які здійснюють або говорять, що здійснюють соціологічні дослідження.

Напередодні кожних виборів кількість суб'єктів, що продукують різні рейтинги, опитування тощо зростає в рази. Їх оприлюднення в ЗМІ починається задовго до офіційного початку передвиборчої агітації. І до 2014 року ці питання залишались поза межами закону. У взаємодії громадянського суспільства і органів державної влади до основних законів про вибори – "Про вибори Президента України" [13], "Про вибори народних депутатів України" [14] та "Про місцеві вибори" [15], було внесено статті 56-6, 67 і 53 відповідно, що мають однакову назву і містять ідентичні положення щодо особливостей поширення інформації про результати опитування громадської думки, пов'язаного з виборами.

З положень цих норм слідує, що існує два основних суб'єкта відносин, що регулюються – підприємства, заклади, установи та організації, що проводять опитування громадської думки, з одного боку, та інформаційні агентства і ЗМІ, що поширюють їх результати, з іншого.

Неоднозначним є перелік суб'єктів, що проводять опитування громадської думки – підприємства, заклади, установи та організації. Чи означає він, що одноосібно фізичною особою, або декількома фізичними особами не може бути проведено опитування? Не передбачено також організаційної форми таких суб'єктів – чи зобов'язані вони мати статус юридичної особи? Також, законодавством України не регулюється питання методології і методики проведення соціологічних досліджень, отже не забороняється застосовувати жодні методи, в тому числі науково неперевірені або такі, автором яких є окрема фізична особа.

Хоча у згаданих нормах передбачено перелік обов'язкової інформації, що має бути зазначена при оприлюдненні результатів опитування громадської думки, пов'язаного з виборами, а саме: часу його проведення, території, яку охоплювало опитування, розміру та способу формування соціологічної вибірки опитаних, методу опитування, точного формулювання питань, можливої статистичної похибки. Цей обов'язок покладено на виконавців опитування, але він стосується також інформаційних агентств і ЗМІ. Додатково, останні зобов'язані оприлюднити повну назву організації, що проводила опитування і замовників опитування. Виникає закономірне питання – якщо сам виконавець не зобов'язаний зазначати замовника опитування, то звідки має отримати таку інформацію інформагентство або ЗМІ?

Під час передвиборчого процесу влітку 2019 року відсутність відповідного правового регулювання уможливила ситуацію, коли чотири провідні соціологічні центри, які отримали запит з вимогою розкрити замовників досліджень електоральних симпатій суспільства, відмовилися оприлюднювати цю інформацію, оскільки закон не зобов'язує їх це робити. Центр демократії та верховенства права надіслав інформаційні запити до Київського міжнародного інституту соціології, Соціологічної групи "Рейтинг", Центра Разумкова та Центру "Соціальний моніторинг" щодо оприлюднення замовників їхніх останніх соцопитувань громадської думки про підтримку політичних партій, аргументуючи тим, що запитувана інформація є суспільно значимою [16].

В цій ситуації виникає ще одна колізія – адже інформація про замовника може бути віднесена до комерційної таємниці, і часто так і є. Тому відповідний виконавець

соціологічного дослідження не лише не зобов'язаний, а й не має права оприлюднювати таку інформацію.

Інформаційні загрози, пов'язані з оприлюдненням результатів опитувань громадської думки.

Способи маніпуляції громадською думкою з використанням результатів соціологічних досліджень дуже розмаїті і залежать від численних чинників – чи проводилось дослідження насправді, чи використана методологія є науковою і дозволяє отримати вірогідні результати, коли і яким чином було оприлюднені результати, яка мета і цільова аудиторія інформаційного впливу тощо.

"Фейкові" дослідження, тобто дослідження яких не було в принципі, або вони є профанацією досліджень. Вже згадані фірми-"одноденки", що виринають перед виборами, не бридяться фальсифікацією як самих опитувань, так і їх результатів. Для їх оприлюднення потужно використовується Інтернет-простір, особливо, соцмережі. Адже обмежений за розміром формат повідомлень у мережі є стандартним, тому не викликає зайвих запитань, коли не містить інформації ані про виконавця дослідження, ані про замовника, а тим паче про саме дослідження.

Проте і у соціологічних дослідженнях, що дійсно проводяться, можливі маніпуляції на всіх етапах. Наприклад, на результат опитування щодо підтримки того чи іншого кандидата може вплинути: хто саме з'являється в переліку, які запитання поставлені і які відповіді запропоновані, чи достатньою є вибірка, чи всі регіони охоплені, чи добросовісні опитувачі. Пересічний громадянин не розуміється і не мусить розумітись на цих тонкощах. Чого не скажеш про політтехнологів і самих соціологів. Закономірно виникає питання про відповідальність журналістів при оприлюдненні результатів.

Адже оприлюднення результатів досліджень може мати абсолютно різний вплив на електорат.

На сторінці інформагентства "Інтерфакс Україна", в рубриці опитування розміщено повідомлення, що "Агентство "Інтерфакс-Україна" не може ні підтвердити, ні поставити під сумнів достовірність наведених даних. Факт публікації їх на сторінці "Опитування" нашого сайту не є свідченням репрезентативності проведеного дослідження" [17]. Таким чином, агентство відмовляється від відповідальності за достовірність поширюваної інформації.

Проведення справжнього соціологічного дослідження науково обґрунтованими методами і в рамках закону вимагає праці фахівців, яка є затратною і у фінансовому, і організаційному вимірі. А навіть фальсифіковані рейтинги і їх оприлюднення в ЗМІ – також не безкоштовні. Хто і чому готовий за це платити?

Суб'єкти, що зацікавлені в проведенні та/або оприлюдненні рейтингів.

Насамперед, рейтинги необхідні для *політичних сил і кандидатів*. Ірина Бекешкіна, директор фонду "Демократичні ініціативи", зазначила: "Рейтинги не так впливають на виборців, як на спонсорів" [17]. Політична боротьба потребує фінансування. Одна лише політична реклама коштує сотні мільйонів гривень. Рейтинг дозволяє визначити спонсору, чи є політик добрим капіталовкладенням.

Для громадянського суспільства. Володимир Фесенко, голова правління Центру прикладних політичних досліджень "Пента", вважає, "на виборців впливають результати соціологічних досліджень за умови, що вони схильні робити раціональний вибір, а не емоційний" [17]. Для виборця, який думає і аналізує інформацію, що споживає, результати соціологічних досліджень, в тому числі рейтинги, їх лідери, зміни

в залежності від об'єктивних подій або ж внаслідок роботи політтехнологів – є добрим харчем для розуму.

Водночас, не слід забувати про іншу сторону медалі. Людям властиво приймати рішення під впливом так званого ефекту натовпу – "куди всі, туди й я". Особливо в пострадянському просторі, де однією з панівних ідеологем залишається віра в те, що інші, особливо, якщо це більшість, знають краще. Це дозволяє використовувати рейтинги як засіб маніпуляції.

Держава не може і не зобов'язана змушувати людей думати і критично сприймати інформацію. Однак, згідно Конституції України кожен громадянин України має право брати участь в управлінні державними справами, зокрема вільно обирати і бути обраними до органів державної влади та органів місцевого самоврядування. Право вільно обирати передбачає не лише відсутність примусу на етапі волевиявлення, а й забезпечення умов для вільного формування своєї волі (порівн. ст. 6 Законів України "Про вибори Президента України", "Про вибори народних депутатів України" та "Про місцеві вибори").

Щоби зробити власний вільний вибір, виборцю має бути забезпечено своєчасний доступ до достовірної і повної інформації, і це є основоположними принципами інформаційних відносин, що визнає ст. 2 Закону України "Про інформацію". Держава ж взяла на себе зобов'язання забезпечувати кожному доступ до інформації і забезпечувати інформаційну безпеку України, складовими якої є інформаційна безпека людини, суспільства і держави.

Зацікавленим державам і міжнародному співтовариству. При цьому, зацікавленість є в різних результатах – демократичних виборах в Україні або доведенні неспроможності демократії, та й взагалі державності в Україні. Одним з основних наративів, що транслює російська пропаганда на захід, є "Україна – неспроможна держава" (англ. – failed state). Така держава видається некерованою й недостатньо легітимною в очах міжнародного співтовариства у зв'язку з розпадом державної влади. Якщо влада нелегітимна (чомусь пригадався один колишній "легітимний"), то з нею треба боротись. А "доброзичлива" підтримка для таких борців надходить швидко і чомусь без розпізнавальних знаків.

Для країн з віковими демократичними традиціями, країн-партнерів України важливо знати, що ж насправді тут відбувається. Міжнародні організації замовляють соціологічні дослідження, як правило, компетентним інституціям з доброю репутацією.

Об'єктивність, вірогідність, повнота і точність інформації відповідно до статті 5 Закону України "Про інформацію" належать до основних принципів інформаційних відносин.

Щодо заборони оприлюднення неправдивих результатів соціологічних досліджень, то відповідно до ст. 47 Закону України "Про інформацію" відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень, як надання інформації, що не відповідає дійсності, поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи.

Проте ст. 6 Закону України "Про оперативно-розшукову діяльність" [19] підстави для проведення оперативно-розшукових заходів з попередження оприлюднення неправдивих результатів соціальних досліджень не передбачено.

Крім того, оприлюднення вигаданих (неправдивих) результатів соціологічних досліджень щодо можливості громадян бути обраними безпосередньо не визначається законодавством України як застосування обману чи будь-яких інших дій, що

перешкоджають вільному формуванню волі виборця, а отже не передбачає відповідальності.

Законодавством України також не встановлено переліку методів збору інформації у процесі опитування громадської думки, пов'язаного з місцевими виборами, порядку визначення статистичної оцінки можливої помилки такого опитування і не забороняється застосовувати методи соціологічного дослідження, автором яких є окрема особа.

Висновки.

1. Цитуючи нобелівського лауреата з економіки і поведінкового психолога Річарда Талера, зазначимо, що "соціально-заразним може бути майже будь-що: від ожиріння до оцінок в університеті, від народжуваності до самогубств" [20]. А це означає що оприлюднення рейтингів кандидатів або інші результати соціологічних досліджень мають безпосередній вплив на формування волі виборців, а отже – на реалізацію їх виборчого права.

2. Держава, яка декларує себе як демократична і правова зобов'язана забезпечувати створення умов для вільного волевиявлення своїх громадян як основу збереження демократичних цінностей в українському суспільстві, а також задля забезпечення національної безпеки.

3. Важливо, що правового регулювання потребує як проведення соціологічних досліджень, так і порядок оприлюднення їх результатів. Необхідним вбачається встановлення відповідальності за дії, що перешкоджають вільному формуванню волі виборця, зокрема, за оприлюднення неправдивих результатів соціологічних досліджень, невиконання вимог законодавства щодо оприлюднення замовника та іншої визначеної законом інформації як ЗМІ, так і виконавцями соціологічних досліджень.

Використана література

1. Богдан О. Що варто знати про соціологію та соціальні дослідження. Київ: Дух і Літера, 2015. 380 с.

2. Жванія Т.В. Електоральна поведінка: теоретичні підходи до вивчення. *Сучасне суспільство*. 2014. Вип. 1. С. 39-49.

3. Звернення Соціологічної Асоціації України. URL: http://kiis.com.ua/?lang=ukr&cat=news&id=816&page=4

4. Тоффлер Э. Метаморфозы власти. Знание, богатство и сила на пороге XXI века. URL: https://royallib.com/book/toffler_elvin/metamorfozi_vlasti.html

5. Мак-Люэн М. Галактика Гутенберга. Становление человека печатающего. Київ: "Ника-Центр", 2003. 432 с.

6. Брижко В.М. та ін. е-боротьба в інформаційних війнах та інформаційне право: монографія; за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. – (НДЦПІ АПрН України). Київ: Видавництво ТОВ "Пан-Тот", 2007 р. 234 с.

7. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право*. 2015. № 2. С. 111-120.

8. Додонов Д.Р. Раціоналізація політичної поведінки в контексті формування демократичного суспільства: автореф. дис. на здобуття наук. ступеня канд. політ. наук: 23.00.03. Київ, 2019. 20 с.

9. Почепцов Г. Пропаганда 2.0. Харків: Фоліо, 2018. 800 с.

10. Поліщук І.О. Політико-правова ментальність українства: концептуально-методологічні засади дослідження. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Політологія*. Харків, 2016. № 2. С. 28-36.

11. Фурашев В.М., Самчинська О.А. Маніпуляції свідомістю людини як основний спосіб ведення передвиборчих кампаній. *Інформація і право*. № 3(30)/2019. С. 119-125.

12. Про інформацію: Закон України від 02.10.92 р. № 2657-12. URL: https://zakon.rada.gov.ua

13. Про вибори Президента України: Закон України від 05.03.99 р. № 474-XIV. URL: https://zakon.rada.gov.ua

14. Про вибори народних депутатів України: Закон України від 17.11.11 р. № 4061-VI. URL: https://zakon.rada.gov.ua

15. Про місцеві вибори: Закон України від 14.07.15 р. 595-VIII. URL: https://zakon.rada.gov.ua

16. ЦЕДЕМ вимагає від чотирьох соціологічних організацій розкрити замовників останніх досліджень. URL: https://vybory.detector.media/2019/07/18/tsedem-vymahaje-vid-chotyroh-sotsiolohichnyh-orhanizatsij-rozkryty-zamovnykiv-ostannih-doslidzhen

17. Соціологія і вибори: аргумент для розумного вибору чи маніпуляції? URL: https://www.ukrinform.ua/rubric-presshall/2629512-sociologia-i-vibori-argument-dla-rozumnogo-vibo ru -ci-manipulacii.html

18. Золотар О.О. Кому потрібні рейтинги CREDO. URL: https://credo.pro/2019/02/229934?

19. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII. URL: https://zakon.rada.gov.ua

20. Талер Р. Поведінкова економіка. Як емоції впливають на економічні рішення / пер. С. Крикуненко. Київ: Наш Формат, 2018. 464 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 343.14:004

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,*
провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України
СЕРЬОГІН В.С., науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України

УДОСКОНАЛЕННЯ МЕТОДИЧНОГО ЗАБЕЗПЕЧЕННЯ ЕКСПЕРТНИХ ДОСЛІДЖЕНЬ СПЕЦІАЛЬНИХ ПРОГРАМНИХ ЗАСОБІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *Стаття присвячена аналізу проблем експертного забезпечення правоохоронної діяльності у сфері протидії кіберзлочинності. В межах статті досліджуються проблемні питання розробки методичних матеріалів для проведення експертних досліджень спеціальних програмних засобів. Запропоновані перспективні напрями подальших наукових досліджень протидії кіберзлочинності, модернізації та вдосконалення методик проведення експертних досліджень спеціальних програмних засобів.*

Ключові слова: *кіберзлочинність, механізм слідоутворення, шкідливі програмні засоби, спеціальний програмний засіб негласного отримання інформації.*

Summary. *The article is devoted to the analysis of the problems of expert support for activities in law enforcement in the field of countering cyber crime. The article examines the problematic issues of the development of methodological materials for the conduct of expert studies of special software. Prospective directions for further research of the problem of countering cyber crime, upgrading and improving the methods of conducting expert studies of special software have been proposed.*

Keywords: *cyber security, tracing mechanism, harmful software, special software for covert obtaining of information.*

Аннотация. *Статья посвящена анализу проблем экспертного обеспечення правоохранительной деятельности в области противодействия киберпреступности. В рамках статьи исследуются проблемные вопросы разработки методических материалов для проведения экспертных исследований специальных программных средств. Предложены перспективные направления дальнейших научных исследований противодействия киберпреступности, модернизации и совершенствования методик проведения экспертных исследований специальных программных средств.*

Ключевые слова: *кибербезопасность, механизм следообразования, вредные програмные средства, специальное программное средство негласного получения информации.*

Постановка проблеми. Сьогодні стрімкий розвиток інформаційних технологій, масштаб застосування глобальних телекомунікаційних мереж, розробка новітніх телекомунікаційних пристроїв створює умови для зростання злочинності у сфері комп'ютерної інформації як в Україні, так і за її межами.

Кіберзлочинність, що пов'язана з використанням інформаційних технологій, комп'ютерних систем та мереж, здатна продукувати такі наслідки, які за масштабом наближаються до техногенної катастрофи чи економічної кризи. У 2008 році щорічна шкода від кіберзлочинності оцінювалася експертами ОБСЄ приблизно у 100 млрд. доларів [1]. Сьогодні ж збитки світової економіки від кіберзлочинності оцінюються у $ 1,5 трлн. на рік, а за негативним сценарієм у 2019 році вони сягатимуть $ 2 трлн. [2].

Революційне зростання кіберзлочинності з використанням сучасних інформаційних технологій на початку XXI століття можна порівняти з появою ядерної зброї, небезпечний руйнівний потенціал якої обумовив впровадження правових підстав її застосування.

Отже, кіберзлочинність є сьогодні однією з найгостріших проблем інформаційної безпеки держави.

Результати аналізу наукових публікацій. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська [3], Ю.М. Батурин [4], П.Д. Біленчук [5], О.В. Ботвінкін [6], В.Д. Гавловський [7], В.О. Голубєв [8], М.В. Карчевський [10; 11], В.В. Поляков [11], М.О. Кравцова, О.М. Литвинов [12], Ю.Ю. Нізовцев [13], Б.В. Романюк [14], О.Р. Росинська [15], Т.Л. Тропіна [16], О.М. Черкун, О.К. Юдін [17] та інші.

Вагомий внесок у розроблення методів, засобів і технологій ідентифікації та фіксації кіберзлочинів внесено дослідженнями, проведеними зарубіжними вченими. Це праці Д. Айкова, К. Сейгера, У. Фонсторха [18], К. Брайана [19] та С. Бренера [20].

Водночас, слід відзначити, що в більшості публікацій, присвячених питанням кіберзлочинності, мають місце неоднозначні судження, різні точки зору, істотні розбіжності між поглядами дослідників з питань методичного забезпечення розслідування комп'ютерних злочинів.

Незважаючи на значну кількість публікацій, що вийшли останнім часом, присвячених проблемам протидії комп'ютерній злочинності, більшість дослідників основну увагу приділяють загальним кримінально-правовим та криміналістичним аспектам цієї проблеми.

Практично не досліджена така важлива галузь теорії, як доведення ознак, обставин, способів вчинення злочинів у сфері комп'ютерної інформації для їх фіксації та ідентифікації, що має важливе значення для розробки методик забезпечення експертних досліджень кіберзлочинів [12, с. 210; 14].

Сьогодні масштаб та рівень кіберзлочинності, поява нових способів і методів кіберзлочинів зумовлює потребу подальших досліджень цієї тематики, спрямованих на удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності.

Метою статті є удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності.

Виклад основного матеріалу. Інформаційна зброя як інструмент кіберзлочинності характеризується такими ознаками, як цілеспрямованість, вибірковість, розосередженість, швидкість доставки, масштабність та досяжність впливу, комплексність впливу на технічні засоби, системи і людей, регулювання (дозування) "потужності" впливу, що зближує її зі зброєю масового ураження.

Підвищення результативності протидії кіберзлочинності безумовно потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях [7, с. 110].

Одним із важливих напрямів забезпечення діяльності правоохоронних органів з розслідування кіберзлочинів є удосконалення нормативно-методичного забезпечення слідчих дій та експертних досліджень стосовно кіберзлочинів, зокрема удосконалення методів і технологій ідентифікації та фіксації кіберзлочинів за результатами практики застосування кримінально-правових норм, що охороняють інформацію в комп'ютерних системах та телекомунікаційних мережах.

Широкий спектр технологій вчинення кіберзлочинів відзначається різноманітністю механізмів слідоутворення з можливістю приховування або змін комп'ютерної інформації щодо слідів злочину, що, в кінцевому результаті, визначають їх високу латентність [17, с. 176].

Зазначені чинники, а також складність виявлення та фіксації комп'ютерної інформації щодо типових слідів здійснення злочинів, встановлення механізму слідоутворення, способу вчинення злочину ускладнюють процес формування криміналістичної характеристики кіберзлочинів та взагалі методів і технологій їх ідентифікації.

В сучасній криміналістиці дослідження застосовуваних засобів та технологій для вчинення кіберзлочинів, їх приховування не досягли практично значущих результатів, які б дозволили розробити як тактико-криміналістичні рекомендації з розслідування таких злочинів, так і методики експертних досліджень у цій сфері [11, с. 162].

Кіберзлочини завжди здійснюються з використанням засобів комп'ютерної техніки. До цих засобів відносяться комп'ютери в різноманітних варіантах їх виконання (ноутбуки, планшети, смартфони, тощо), комп'ютерні технології (бездротові Wi-Fi, Bluetooth, WiMAX тощо), а також комп'ютерне програмне забезпечення як загального використання, наприклад, Opera, Mozilla Firefox, так і програмне забезпечення, використання якого заборонено, наприклад, SpyEye, Zeus, Carberp тощо [11, с. 162].

Слід зазначити, що важливу роль при вчиненні сучасних кіберзлочинів виконує саме спеціально розроблене програмне забезпечення.

Як свідчить сучасна практика слідчих дій, в переважній більшості випадків кіберзлочини (кібертероризм, кібершпигунство) здійснюються шляхом віддаленого несанкціонованого доступу до комп'ютерів, комп'ютерних систем, комп'ютерних мереж та мереж електрозв'язку за допомогою комп'ютерної техніки загального використання, на яку встановлюється спеціальне програмне забезпечення, наприклад, Dugu, Wiper, Flame, Gauss, Madi, Narilam [11, с. 164].

Зауважимо, що шкідливі програмні та технічні засоби, призначені для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку є предметом злочину, передбаченого ст. 361-1 "Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут" КК України.

До речі, питання щодо співвідношення понять "предмет" і "засоби або знаряддя вчинення злочину" кримінально-правовою науковою не зовсім вирішене, оскільки матеріальні утворення, що не підпадають під поняття "предмет злочину", належать не до об'єкта, а до об'єктивної сторони складу злочину. Основним універсальним критерієм відмежування "предмет злочину" від поняття "знаряддя та інші засоби вчинення злочину" дослідники цієї проблеми визнають те, що засоби – це речі, за допомогою яких суб'єкт прагне досягти злочинного результату. Предмет сам піддається злочинному впливу [21, с. 137]. Обов'язковою ознакою предмету розглядуваного злочину є те, що за своїм призначенням шкідливі програмні засоби мають несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Відсутність цієї ознаки виключає можливість визнати вказані програмні чи технічні засоби як предмет злочину, передбаченого ст. 361-1 КК України [10].

Несанкціоноване втручання в роботу комп'ютерів, комп'ютерних систем чи мереж, слід розуміти, як проникнення до цих комп'ютерів, систем чи мереж, злом їх засобів програмно-апаратного захисту інформації, отримання доступу до управління

комп'ютером, комп'ютерної системи чи мережі, а також до комп'ютерної інформації, що може призвести до витоку, втрати, підробки, блокування цієї інформації, спотворення процесу обробки інформації в комп'ютері, комп'ютерних системах чи мережах, без дозволу (згоди) відповідного власника або уповноважених ним осіб [10].

Злочин, передбачений ч. 1 ст. 361-1 КК України, є злочином з формальним складом, тому для наявності його об'єктивної сторони не потрібно встановлювати настання суспільно небезпечних наслідків [10].

Наведені чинники, а також складність виявлення та фіксації слідів несанкціонованого проникнення до комп'ютерів, систем чи мереж, злому їх засобів програмно-апаратного захисту інформації ускладнюють формування методів ідентифікації шкідливих програмних засобів та методичного забезпечення їх експертних досліджень.

Сьогодні в спеціалізованих експертних установах України впроваджені методичні матеріали для забезпечення проведення досліджень носіїв цифрової інформації та комп'ютерної інформації, які використовуються у тому числі й для методичного забезпечення дослідження програмних засобів [22 – 25]. Зазначені методики, а також методичні рекомендації зарубіжних вчених [18 – 20] передбачають єдиний методичний підхід до процесів огляду, фіксації стану речових доказів (збереження, копіювання даних, що знаходяться на наданих на дослідження носіях інформації) та дослідження цифрової інформації, що розміщується на них, оформлення матеріалів експертного дослідження. При цьому, рекомендовані методи дослідження комп'ютерної інформації та технології контролю активності досліджуваних програмних засобів (далі – ПЗ) можуть бути застосовані для виявлення слідів реалізації його функцій [25].

Встановлення та оцінка сукупності слідів дозволяє виявити функції шкідливого програмного засобу, що забезпечують здійснення несанкціонованого доступу до управління комп'ютером та комп'ютерної інформації [23; 25].

Такий підхід дозволяє вирішити діагностичну задачу при проведенні досліджень ПЗ, яка спрямована на встановлення загальної характеристики програмного засобу та визначення його недокументованих функцій, які забезпечують виконання злочинних дій.

На жаль, сьогодні практично не досліджено такий важливий розділ криміналістичної теорії, потенціал якого пояснює підходи щодо доведення ознак (типових слідів несанкціонованого втручання), способів несанкціонованого втручання в роботу комп'ютерів, комп'ютерних систем чи мереж (проникнення до цих комп'ютерів, систем чи мереж, злом їх засобів програмно-апаратного захисту інформації), що має важливе значення для визначення призначеності програмних засобів та їх належності до шкідливих програмних засобів.

Під час розробки методів ідентифікації та фіксації кіберзлочинів слід враховувати особливості функціональних можливостей різноманітних шкідливих програмних засобів (далі – ШПЗ) та їх класифікацію.

З точки зору криміналістики дослідження засобів вчинення кіберзлочинів, їх типізація та класифікація дозволять встановити причинові зв'язки між обставинами, що підлягають встановленню та доведенню під час слідчих дій та експертних досліджень [11, с. 162-163].

Сьогодні найбільш поширеною є розроблена на базі запропонованої "Лабораторією Касперського" класифікація, яка сформована з урахуванням особливостей функціональних можливостей ШПЗ, котрі визначають технологію їх застосування [10, с. 512].

Зазначена класифікація спрямована на забезпечення функціонування засобів програмно-апаратного захисту інформації, що циркулює в комп'ютерах, комп'ютерних системах, мережах та мережах електрозв'язку.

За технологією застосування виділяють такі види шкідливих програмних засобів: класичні комп'ютерні віруси; мережеві черв'яки; трояни; руткіти.

До окремого підвиду ШПЗ належить шпигунське програмне забезпечення (Spyware), яке призначене для незаконного віддаленого доступу до управління комп'ютером та комп'ютерної інформації.

За результатами аналізу шляхів еволюції їх застосування можна дійти висновку, що сучасні ШПЗ – це високотехнологічні програмні засоби, що спеціально розробляються для застосування іноземними спецслужбами, в якості кіберзброї, при проведенні спецоперацій за конкретними об'єктами посягання [13, с. 232].

При цьому вибір засобів для здійснення кіберзлочинів звичайно залежить від цілого ряду факторів: технологічної інфраструктури об'єкта посягання та прийнятого на ньому режиму охорони (застосовуваних технічних і організаційних засобів охорони, програмно-апаратного захисту інформації). Сучасні ШПЗ розробляються за цільовим призначенням як програмні комплекси, що складаються з взаємопов'язаних програмних додатків, які забезпечують виконання функціональних завдань на певних стадіях підготовки до вчинення злочину, безпосередньо при його здійсненні та при приховуванні злочину, наприклад, Stuxnet, BlackEnergy [11, с. 164].

Тому одним з пріоритетних напрямів протидії кіберзлочинності, зокрема запобігання застосуванню іноземними спецслужбами високотехнологічних програмних засобів, вважається здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на запобігання та припинення злочинної діяльності щодо створення, розповсюдження або збуту зазначеного спеціального програмного забезпечення.

Органи досудового розслідування, особливо на первісному етапі розслідування комп'ютерних злочинів, рідко мають вичерпні відомості про засоби, що використовуються під час вчинення злочину.

За відсутності такої інформації важливу роль для проведення розслідування має класифікація спеціальних програмних засобів, яка може бути сформована з урахуванням криміналістичної характеристики схожих злочинів. Її практичне значення, що проявляється в кореляційному взаємозв'язку між структурними елементами злочину, дає підстави для підготовки слідчих версій за наявності лише неповних отриманих даних [11, с. 163].

Отже, одним з актуальних досліджень нормативно-методичного забезпечення протидії кіберзлочинності є розробка класифікації спеціальних програмних засобів, яка сформована з використанням криміналістичної характеристики схожих злочинів.

Враховуючи актуальність питань протидії незаконному обігу спеціальних програмних засобів (так званих "шпигунських" програм), які дозволяють ефективно здійснювати дії з віддаленого доступу та негласного отримання інформації з абонентських та інших телекомунікаційних пристроїв телекомунікаційних мереж, в ІСТЕ СБ України було розроблено методичні рекомендації для проведення експертних досліджень програмних засобів, призначених для негласного отримання інформації (далі – ПЗ НОІ) [26].

Слід підкреслити, що віднесення програмного засобу до предмету згаданого злочину потребує встановлення за результатами дослідження необхідної сукупності ознак та властивостей, які є достатніми для визначення його призначеності для негласного отримання інформації.

На відміну від вказаних методів дослідження комп'ютерної інформації, дослідження ПЗ НОІ повинно передбачати як аналіз слідів (ознак) реалізації функціоналу програмного засобу, так і безпосереднє дослідження дій комп'ютера чи телекомунікаційного пристрою, на який встановлено програмний засіб, з визначенням причинових зв'язків між виявленими діями з негласного отримання інформації та функціями ПЗ [26].

Розроблення методичних рекомендацій "Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації" базується на критеріях віднесення технічних та програмних засобів до спеціальних технічних засобів негласного отримання інформації та методичних матеріалів зарубіжних і вітчизняних фахівців у сфері комп'ютерно-технічної експертизи [19; 20; 22 – 25].

Новизною методичних рекомендацій є запропонований підхід щодо дослідження ПЗ, який передбачає комплексне застосування різних методів досліджень, зокрема методів контролю активності ПЗ та виконання відповідних видів експертних задач як в галузі комп'ютерно-технічної експертизи, так і в галузі експертизи СТЗ [26].

Предметом експертних досліджень ПЗ є факти й обставини, виявлені при дослідженні використання програмних засобів, що встановлені на технічні засоби загального користування (комп'ютери, телекомунікаційні пристрої тощо) та забезпечують реалізацію інформаційних процесів.

Аналіз результатів досліджень слідів реалізації функцій ПЗ, дій телекомунікаційного пристрою з негласного отримання інформації, на який встановлено ПЗ, та виявлених причинових зв'язків між ними, дає підстави для:

– визначення можливості здійснення негласного отримання інформації з використанням наданого на дослідження програмного засобу;

– віднесення програмного засобу до ПЗ НОІ [26].

Під об'єктом експертних досліджень ПЗ слід розуміти прикладне програмне забезпечення, що знаходиться на наданих носіях інформації, або інстальоване на технічних засобах загального користування, а також інформаційні процеси, які обумовлені функціонуванням зазначених технічних засобів загального користування.

При цьому залишається задача дослідження ПЗ за відсутності вихідних кодів, що значно ускладнює роботу дослідника [25].

Як правило, при проведенні експертного дослідження вирішуються діагностичні та ситуаційні задачі, а також задачі групофікації ПЗ. При проведенні досліджень ПЗ діагностичні задачі спрямовані на:

– встановлення загальної характеристики програмного засобу, з яких файлів та каталогів він складається, їх параметрів (обсяг, атрибути тощо);

– визначення функцій програмного засобу, які забезпечують виконання певних дій з негласного отримання інформації;

– встановлення типів апаратно-програмних платформ, що підтримують функціонування програмного засобу.

Серед ситуаційних задач виділяється зняття процесів (одномоментних станів) у режимі реального часу, встановлення й сприйняття яких можливо тільки з використанням спеціалізованих програмних засобів або в певних умовах (наприклад, у складі певної конфігурації технологічного устаткування, у складі комп'ютерної системи або мережі тощо).

Під час виявлення ознак функціонування спеціального програмного засобу на підставі аналізу процесів у режимі реального часу звертається увага на:

– читання/запис даних у файловій системі – створення, видалення, редагування файлів, каталогів,

– дописування інформації в файл;

– модифікації пам'яті – створення чи завершення процесів, створення прихованих процесів;

– зміни реєстру – створення нових записів в реєстрі, редагування або видалення існуючих;

– зовнішню мережеву активність – отримання чи відсилання інформації через мережу;

– внутрішню мережеву активність – отримання чи відсилання інформації через localhost;

– перехоплення хуків клавіатури;

– відкриття портів;

– запуск файлів в операційній системі;

– встановлення чи заміну драйверів [26].

Для виявлення ознак функціонування спеціального програмного засобу, інстальованого на технічних засобах загального користування, використовується спеціалізоване програмне забезпечення, наприклад, ThreatExpert, Process Monitor, Defense Wall HIPS, SafenSoft SysWatch Deluxe. При використанні зазначеного програмного забезпечення застосовується один з трьох основних методів контролю активності ПЗ: HIPS, VIPS та Пісочниця (sandbox) [25]. Найбільш часто застосовується метод контролю активності ПЗ HIPS, який має наступні переваги:

– низьке споживання системних ресурсів;

– невимогливі до апаратного забезпечення ПК (можуть працювати на різних платформах);

– можливість визначення загроз нульового дня;

– можливість визначення руткітів, які працюють в режимі користувача.

Технологія HIPS – це технологія контролю активності, заснована на перехопленні звернень до ядра ОС і блокуванні виконання потенційно небезпечних дій ПЗ, яке працює в режимі користувача, виконуваних без відома користувача [25]. За допомогою власного драйвера перехоплює всі звернення ПЗ до ядра ОС. У разі спроби здійснення потенційно небезпечної дії з боку ПЗ, HIPS-система блокує виконання даної дії і запитує користувача, який вирішує дозволити або заборонити виконання цієї дії.

При проведенні досліджень ПЗ на стадії експертного експерименту вирішення ситуаційної задачі полягає в оцінці можливостей виконання певних дій з негласного отримання інформації та виявлення необхідної сукупності функцій ПЗ, які є достатніми для визначення його функціонального призначення.

Дослідження програмного засобу в реальних умовах його функціонування може бути організовано на базі технології "клієнт-сервер" телекомунікаційно-інформаційної системи, яка включає пункт управління об'єднаний телекомунікаційною мережею з абонентськими пристроями, на яких здійснюється перехоплення та передача дистанційно встановлених видів інформації.

Експертні задачі на стадії порівняльного дослідження ПЗ спрямовані на встановлення його групової належності до спеціальних програмних засобів, призначених для негласного отримання інформації (як різновиду спеціальних технічних засобів негласного отримання інформації).

Запропонована в методичних рекомендаціях процедура аналізу виявлених функцій ПЗ з урахуванням встановлених в методичних рекомендаціях суттєвих ознак (функціональних можливостей) ПЗ НОІ дозволяє з'ясувати спосіб функціонування ПЗ, його властивості з негласного отримання інформації, а також визначити, в кінцевому підсумку, призначеність програмного засобу [26].

Висновок щодо віднесення ПЗ до ПЗ НОІ формується відповідно до встановлених критеріїв, а саме – наявності загальних (критеріальних) ознак програмного засобу: придатності програмного засобу для негласного отримання інформації та призначеності програмного засобу для його застосування у прихований спосіб, який характерний для оперативно-розшукових заходів [26; 27].

Висновки.

Актуальність проблеми протидії кіберзлочинності в умовах сьогодення потребує системного вирішення питань її забезпечення на законодавчому, організаційному та нормативно-методичному рівнях.

Проблема удосконалення методичного забезпечення правоохоронної та експертної діяльності в сфері боротьби з кіберзлочинністю зумовлює необхідність розробки класифікації кіберзлочинів, тактики проведення слідчих дій з їх розслідування та фіксації, методик та ефективних методів, спрямованих на удосконалення ідентифікації спеціального програмного забезпечення, що призначено для незаконного віддаленого доступу до управління комп'ютером та комп'ютерної інформації. Одним із важливих напрямів удосконалення методичного забезпечення протидії кіберзлочинності є впровадження методичних матеріалів для забезпечення проведення експертних досліджень спеціальних програмних засобів, призначених для негласного отримання інформації.

Запропоновані рекомендації експертного дослідження програмних засобів, критерії їх віднесення до ПЗ НОІ можуть слугувати підґрунтям для розробки методик проведення судових експертиз спеціальних програмних засобів незаконного віддаленого доступу до управління комп'ютером, комп'ютерної системи чи мережі, негласного отримання інформації, а також удосконалення методів їх ідентифікації.

Використана література

1. Киберпреступность страшнее финансового кризиса. URL: https://www.crime-research.ru/news/03.12.2008/50 (дата звернення 03.05.2019).

2. Киберпреступники наживаются на самых бедных. URL: https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.html (дата звернення 19.02.2019).

3. Ахтирська Н. Форми протидії розслідуванню злочинів, вчинених у сфері комп'ютерних технологій. *Юридичний журнал*. 2002. № 3(9). С. 60-64.

4. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. Москва: Юридическая литература, 1991. 157 с.

5. Біленчук П.Д., Бут В.В., Гавловський В.Д., Гуцалюк М.В., Колпак Р.Л. Комп'ютерна злочинність: навч. посіб. Київ: Атіка, 2002. 240 с.

6. Ботвінкін О.В. Проблеми забезпечення національної безпеки в інформаційній сфері. *Юридичний журнал.* 2007. № 2. С. 59-60.

7. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. № 1(28)/2019. С. 108-117.

8. Голубєв В.О. Правові проблеми захисту інформаційних технологій. *Вісник Запорізького юридичного інституту*. 1997. № 2. С. 35-40.

9. Карчевский Н.В. Киберпреступление или преступление в сфере использования информационных технологий?: матеріали всеукр. наук.-практ. конф. *Кібербезпека в Україні: правові та організаційні питання*, м. Одеса, 21 жовтня 2016 р. Одеса: ОДУВС, 2016. С. 10-14.

10. Карчевський М.В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2012. 528 с.

11. Поляков В.В., Лапин С.А. Средства совершения компьютерных преступлений: доклады ТУСУРа. 2014. № 2(32). Барнаул: Изд-во Алт. ун-та, 2014. С. 162-165.

12. Кравцова М.О., Литвинов О.М. Запобігання кіберзлочинності в Україні: монографія. Харків: Панов, 2016. 212 с.

13. Нізовцев Ю.Ю. Еволюція шкідливих програмних засобів та аналіз тенденцій небезпеки їх застосування: *зб. наукових праць Національної академії СБ України*. 2017. № 65. С. 230-238.

14. Романюк Б.В., Гавловський В.Д., Гуцалюк М.В., Бутузов В.М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій. Київ: Вид. Поливода А.В., 2004. 144 с.

15. Россинская Е.Р., Усов А.И. Судебная компьютерно-техническая експертиза. Москва: Право и закон, 2001. 416 с.

16. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы / Т.Л. Тропина: дис. …канд. юрид. наук: спец. 12.00.08. Владивосток, 2005. 235 с.

17. Юдин О.К. Інформаційна безпека. Нормативно-правове забезпечення. Киів, 2010. 708 с.

18. Айков Д., Сейгер К., Фонстрох У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Москва: Мир, 1999. 351 с.

19. Для профессионалов криминалистический анализ файловых систем / под ред. Брайана Кэрриэ. С-Пб.: Питер, 2007. 480 с.

20. Brenner S. Cybercrime: criminal threats from cyberspace. Praeger, 2006. 281 p.

21. Кримінальне право України: заг. частина. гл. 7/ за ред. проф. В.В. Сташиса, В.Я. Тація. Харків: Право, 2010. 449 с.

22. Бобрицький С.М., Чишкало О.В. та ін. Дослідження інформації на цифрових носіях (методика): звіт про науково-досліду роботу / Харків: ХНДІСЕ. 2009. 34 с.

23. Усков К.Ю., Пешехонова О.М., Бєляк Ю.М., Кореньок В.А, Ружинський А.О. Методика дослідження комп'ютерної інформації. Київ: КНДІСЕ. 2005. 37 с.

24 Башкатов О., Дружинін Г. та ін. Розробка спеціальних програмних засобів для проведення судових експертиз комп'ютерних мереж / Донецьк: ДНДІСЕ. 2010. 179 с.

25. Войтович О.П., Вітюк В.О., Каплун В.А. Особливості дослідження ознак шкідливого програмного забезпечення без наявності вихідних кодів. *Інформаційні технології та комп'ютерна інженерія*. 2013. № 3. С. 4-9.

26. Дослідження програмних засобів щодо їх віднесення до спеціальних технічних засобів негласного отримання інформації: методичні рекомендації. Київ: ІСТЕ СБУ. 2016. 31 с.

27. Методика віднесення об'єктів до спеціальних технічних засобів негласного отримання інформації. Київ: ІСТЕ СБУ. 2011. 26 с.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 342.52

ПЕТРОВ С.Г., *кандидат юридичних наук,* СБ України

ПРАВОВІ ОСНОВИ ВЗАЄМОДІЇ ДЕРЖАВНИХ ОРГАНІВ ТА ПРИВАТНИХ СУБ'ЄКТІВ ІЗ МЕТОЮ ЗАХИСТУ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ УКРАЇНИ

Анотація. *У статті досліджуються питання взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки і зокрема захисту електронних інформаційних ресурсів України. З цією метою здійснено аналіз підходів в іноземних країнах, а також вітчизняного законодавства.*

Ключові слова*: кібербезпека, взаємодія, правові основи, електронні інформаційні ресурси України, державно-приватна взаємодія.*

Summary. *The article deals with the issues of interaction between public authorities and private entities with the aim of ensuring cybersecurity and protection of electronic information resources of Ukraine in particular. To this end, an analysis of approaches in foreign countries as well as domestic legislation, was carried out.*

Keywords*: Cybersecurity, Interaction, Legal Framework, Electronic Information Resources of Ukraine, Public-Private Interaction.*

Аннотация. *В статье исследуются вопросы взаимодействия государственных органов и частных субъектов с целью обеспечения кибербезопасности и в частности защиты электронных информационных ресурсов Украины. С этой целью осуществлен анализ подходов в иностранных государствах, а также отечественного законодательства.*

Ключевые слова: *кибербезопасность, взаимодействие, правовые основания, государственные электронные информационные ресурсы, государственно-частное взаимодействие.*

Постановка проблеми. Розвиток інформаційних технологій зумовлює розширення загроз безпеці України у сфері обігу державних електронних інформаційних ресурсів. Поширення фактів несанкціонованого доступу до таких відомостей, викрадення інформації з баз даних, знищення та модифікація даних у інформаційних системах, перехоплення інформації тощо зумовлює необхідність наукового обґрунтування питань взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України.

Стратегія кібербезпеки України передбачає необхідність взаємодії з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об'єднань, а також підприємств, установ та організацій незалежно від форми власності, які провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури [1]. Питання ж захисту електронних інформаційних ресурсів України безпосередньо пов'язане із проблемою взаємодії державних і приватних суб'єктів у сфері кібербезпеки.

Результати аналізу наукових публікацій свідчать про те, що питання діяльності СБ України у сфері забезпечення інформаційної безпеки держави було предметом досліджень багатьох українських учених, а саме М.М. Галамби, 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.

Питання взаємодії державного та приватного секторів у сфері кібербезпеки ще у 2014 році аналізували вітчизняні дослідники А.І. Марущак та В.М. Панченко з урахуванням іноземного досвіду і перспектив його використання для України [2].

І.Б. Жиляєв і А.І. Семенченко роблять акцент на необхідності врахування процесів децентралізації та деконцентрації влади, а також фінансово-економічних механізмів [3].

В.В. Круглов пропонує нове розуміння сектору безпеки як спільного підходу держави, приватного сектору та громадян, визначаючи одним із вирішень проблем кібербезпеки "використання моделей державно-приватного партнерства" [4].

Дослідники також звертають увагу на суто практичні питання державно-приватної взаємодії, наприклад, у контексті використання судових експертів задля попередження, виявлення та розслідування кіберзлочинів [5].

Останні наукові роботи з дотичної тематики визначають найбільш перспективними напрямами розвитку національної системи кіберзахисту, зокрема "створення довірчих відносин між державою та суспільством, для якого держава повинна грати сервісну роль" [6, с. 106].

Проблематика державно-приватного партнерства для управління кіберзахистом і запобігання кіберзагрозам в умовах кризових ситуацій, надзвичайного стану, в особливий період актуалізувалося також у рекомендаціях парламентських слухань "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України", у 2016 році [7].

Загалом, як бачимо, питання визначення правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України були предметом досліджень тільки частково.

Метою статті є розкриття правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України.

Виклад основного матеріалу. Насамперед, звернемо увагу на підходи в іноземних країнах до питань взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки загалом і захисту електронних інформаційних ресурсів зокрема. Національна стратегія захисту кіберпростору США, наприклад, окрім іншого визначає заходи, які мають зробити як урядові структури, так і приватні підприємства й користувачі для досягнення безпеки кіберпростору США [8]. Департамент внутрішньої безпеки США використовує програму Automated Indicator Sharing (AIS), яка забезпечує автоматизований обмін даними між державним і приватним секторами задля виявлення і локалізації кіберзагроз і кіберінцидентів [9]. Водночас, як вірно зазначають дослідники НІСД, така взаємодія, поряд із позитивними характеристиками, "викликає… занепокоєння з боку представників приватних компаній через односпрямованість інформаційного обміну, надмірну закритість державних органів" [10].

Подібна неоднозначність спостерігається і в Німеччині, де державно-приватне партнерство спрямоване "на встановлення взаємовигідних правил гри для операторів критично важливої інфраструктури", однак "значна кількість питань (особливо у сфері партнерства щодо об'єктів критичної інфраструктури) об'єктивно залишається невирішеною" [10].

Звернемо увагу на наукову роботу М. Карр і О. Бурес, у яких пропонується запроваджувати ринковий підхід до кібербезпеки у формі державно-приватного партнерства [11, с. 299]. Адже подібний підхід впроваджується у Великій Британії з акцентом на заходи посилення взаємної довіри у межах механізму державних закупівель, а також у забезпеченні державних структур якісними послугами у сфері цифрових технологій [10]. Зважаючи на виділення 1,9 млрд фунтів стерлінгів на

п’ятирічну стратегію кібербезпеки та відкриття Національного Центру кібербезпеки Великої Британії [12], питання взаємодії отримують належне фінансове підґрунтя.

Акцент на співпрацю державних органів з приватним сектором як засіб боротьби з он-лайн-злочинністю роблять і дослідники приватно-публічного партнерства в ЄС [13]. Дійсно, з 2013 року Стратегія кібербезпеки ЄС підкреслює роль взаємодії держави і приватного сектора в боротьбі з кібератаками і кіберзлочинністю [14]. Стратегія єдиного цифрового ринку 2015 р. [15] та Директива ЄС щодо мережевої та інформаційної безпеки [16], яка вступила в силу у серпні 2016 року, поглибили таку взаємодію. А Директива ЄС 2016/1148 від 6 червня 2016 року про заходи щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у ЄС [17] додала вимоги щодо окремих напрямів подібної взаємодії.

Перейдемо до розгляду вітчизняного законодавства щодо досліджуваного питання. Закон України “Про основні засади забезпечення кібербезпеки України” [18, ст. 10] регламентує питання державно-приватної взаємодії у сфері кібербезпеки. Однак, по-перше, зміст поняття “державно-приватна взаємодія” не повною мірою узгоджується з поняттям “державно-приватне партнерство”, закріпленим у Законі України “Про державно-приватне партнерство”. Відповідно, як вірно зазначають представники Національного інституту стратегічних досліджень (далі – НІСД), “не зрозуміло, чи є така взаємодія різновидом державно-приватного партнерства… і чи потрапляє вона під його дію” [10]. По-друге, механізми такої взаємодії і їх особливості для сфери кібербезпеки чітко не виписані.

Якщо державно-приватна взаємодія у сфері кібербезпеки є видом державно-приватного партнерства, то мають “спрацьовувати основні постулати відповідного механізму, наприклад, надання прав управління (користування, експлуатації) об’єктом партнерства або придбання, створення (будівництво, реконструкція, модернізація) об'єкта партнерства з подальшим управлінням (користуванням, експлуатацією), за умови прийняття та виконання приватним партнером інвестиційних зобов’язань відповідно до договору, укладеного в рамках державно-приватного партнерства; фіксація у договірних відносинах “державного інтересу”; довгостроковість відносин (від 5 до 50 років); передача приватному партнеру частини ризиків у процесі здійснення державно-приватного партнерства тощо [19].

Якщо ж державно-приватна взаємодія є іншим за змістом поняттям, то відповідні відносини потребують регулювання іншими правовими нормами. Зважаючи ж на особливості такої взаємодії у сфері кібербезпеки загалом і захисту державних електронних інформаційних ресурсів зокрема, потребує визначення не тільки відповідна термінологія, а й питання обміну даними про кіберінциденти та кібератаки, стандартів кібербезпеки, державних/приватних вимог до сертифікації відповідного обладнання та рішень тощо.

Висловимо позицію про те, що за відсутності закону про кіберзахист критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не можуть бути урегульовані належним чином. Безумовно, прийняття Загальних вимог до кіберзахисту об’єктів критичної інфраструктури [20] є позитивним кроком до створення підґрунтя для державно-приватної взаємодії у сфері кібербезпеки, однак видається за необхідне врегулювання відповідних питань на рівні закону, за попереднім узгодженням із приватними суб’єктами правових механізмів взаємодії (наприклад, участі т.зв. “білих хакерів” у захисті державних та приватних інтересів) та наданням їм певних повноважень і, можливо, преференцій.

Відзначимо активну позицію громадянського суспільства і представників ІТ-бізнесу у налагодженні плідної взаємовигідної співпраці у сфері кібербезпеки. Так, наприклад, Інтернет Асоціація України (ІнАУ) у 2018 році виступила ініціатором "Меморандуму порозуміння про взаємодію у боротьбі з кіберзлочинністю та злочинами, пов'язаними з цифровими доказами", який мав бути підписаний між Нацполіцією України, СБ України, РНБО України та ІнАУ й іншими представниками ринку телекомунікацій [21]. Безумовно, такий крок є важливим для розвитку державно-приватної взаємодії у сфері кібербезпеки в Україні, хоча на сьогодні зазначений Меморандум ще не підписаний.

За наявності неоднозначності у правовому регулюванні питань державно-приватної взаємодії існують непоодинокі приклади практики формування відповідних відносин. Так, зокрема, у Службі безпеки України розроблена і застосовується платформа для збирання, обробки та обміну інформацією про інциденти кібербезпеки, а також технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури в режимі реального часу – "Malware Information Sharing Platform" (MISP). З розпорядниками окремих об'єктів критичної інфраструктури підписані Меморандуми щодо надання доступу до інформаційної системи MISP-UA з метою обміну ідентифікаторами компрометації, що використовувались у кібератаках.

Крім того, за ініціативи СБ України започатковано проект CyberCrime@EAPIII спільно з Радою Європи, який серед іншого спрямований на покращення співробітництва правоохоронних і спеціальних органів країн-членів Східного партнерства з приватним ІТ-сектором у сфері використання електронних доказів у досудових розслідуваннях і протидії кіберзагрозам загалом.

Подібну активність у сфері взаємодії державних органів та приватних суб'єктів демонструють і МВС України, яке у 2015 році підписало Меморандум про взаєморозуміння з корпорацією "Майкрософт" щодо захисту даних, інформаційної та кібербезпеки.

Особливо високу динаміку розвитку КДПП демонструє Департамент кіберполіції Національної поліції України, який залучає експертів для обміну даними, проведення тренінгів для співробітників, взаємодіє з академічною спільнотою, наприклад, Харківським національним університетом радіоелектроніки, Національним аерокосмічним університетом ім. М.Є. Жуковського "ХАІ".

Інший суб'єкт Національної системи кібербезпеки – Національний банк України створив Центр кіберзахисту (CSIRT-NBU), на базі якого долучає представників банківської спільноти до питань формування критеріїв та методології віднесення об'єктів критичної інфраструктури банківської системи України до критичної інфраструктури та вирішення питань організації кіберзахисту в банківській системі України.

Підсумовуючи проведений аналіз, відзначимо, що розвиток правових основ взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів у загальному питанні кібербезпеки потребує, насамперед, запровадження змістовного діалогу як суб'єктів Національної системи кібербезпеки, так і представників ІТ-бізнесу. Такий діалог має бути спрямований на підвищення довіри між приватними суб'єктами та державними органами. У процесі такого діалогу мають використовуватися вже апробовані договірні і правові механізми США, країн ЄС щодо обміну інформацією про позиції та інтереси учасників, зокрема і визначення можливості формування недержавних регуляторних органів, формування системних підходів до підготовки і підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів тощо.

Виконання приватними компаніями державних контрактів щодо підтримки рішень з електронного урядування, документообігу тощо зумовлюють необхідність розподілу обов'язків щодо захисту державних електронних інформаційних ресурсів. Крім того, під час кібератак об'єктами є як державні, так і недержавні ресурси, що зумовлює спільність інтересів при розслідуванні атак. Безумовно, приватні суб'єкти мають сумніви стосовно відкриття доступу до власної інформації з обмеженим доступом, намагаючись проводити внутрішні розслідування інцидентів і кібератак. Актуальними для приватного сектору є й репутаційні ризики, пов'язані з витоком інформації про ненадійність систем захисту на підприємстві. Саме ці питання мають стати предметом попереднього обговорення з наступним їх відображенням у нормах права.

Пропонуємо організувати відповідну платформу для обговорення питань взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Висновки.

Аналіз підходів в іноземних країнах до питань взаємодії державних органів та приватних суб'єктів із метою забезпечення кібербезпеки загалом і захисту електронних інформаційних ресурсів зокрема, а також вітчизняного законодавства щодо досліджуваного питання дав підстави для наступних висновків.

Вважаємо за необхідність узгодження змісту поняття "державно-приватна взаємодія" з поняттям "державно-приватне партнерство". Пропонується при визначенні державно-приватної взаємодії звертати увагу на більш чітку термінологію щодо обміну даними про кіберінциденти та кібератаки, а також наявність більш детальних стандартів у державно/приватних вимогах до сертифікації відповідного обладнання.

Вважаємо, що за відсутності закону про кіберзахист критичної інформаційної інфраструктури, питання державно-приватної взаємодії у сфері кібербезпеки не можуть бути урегульовані належним чином.

Також вважаємо за необхідність запровадити змістовний діалог як суб'єктів Національної системи кібербезпеки, так і представників ІТ-бізнесу з метою підвищення довіри між приватними суб'єктами та державними органами з використанням апробованих договірних і правових механізмів США, країн ЄС щодо обміну інформації про позиції та інтереси учасників, зокрема і визначення можливості формування недержавних регуляторних органів, формування системних підходів до підготовки і підвищення кваліфікації кадрів як державних, так і недержавних суб'єктів тощо.

Відповідну платформу для обговорення пропонується організувати на базі Апарату РНБО України із залученням широкого кола представників державних органів, ІТ-бізнесу, академічного середовища.

Перспективами подальших наукових пошуків визначаємо питання напрацювання правових механізмів взаємодії державних і недержавних суб'єктів у сфері кібербезпеки.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України": Указ Президента України від 15.03.16 р. № 96/2016. *Офіційний вісник України*. 2016. № 23. Ст. 899.

2. Марущак А.І., Панченко В.М. Взаємодія державного та приватного секторів у сфері кібернетичної безпеки: іноземний досвід та перспективи для України. *Інформаційна безпека людини, суспільства, держави*. 2014. № 3 (16). С. 63-79.

3. Жиляєв І.Б., Семенченко А.І. Організаційно-правові механізми розвитку національної системи кібербезпеки України: стан та перспективи. *Стратегічні пріоритети*. 2017. № 4. С. 55-63. URL: http://nbuv.gov.ua/UJRN/spa_2017_4_8

4. Круглов В.В. Державно-приватне партнерство у сфері кібербезпеки. *Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія: Державне управління*. 2018. Т. 29(68). № 3. С. 57-61. URL: http://nbuv.gov.ua/UJRN/sntvupa_2018_29_3_13

5. Русецький А.А. Місце судових експертиз у системі протидії кіберзагрозам у сфері інформаційної безпеки України. *Теорія та практика судової експертизи і криміналістики*. 2018. Вип. 18. С. 263-271. URL: http://nbuv.gov.ua/UJRN/Tpsek_2018_18_32

6. Бакалінська О., Бакалинський О. Правове забезпечення кібербезпеки в Україні. *Підприємництво, господарство і право*. 2019. № 9. С. 100-108.

7. Про Рекомендації парламентських слухань "Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України": Постанова Верховної Ради України. *Відомості Верховної Ради*. 2016. № 17. Ст. 191.

8. National Strategy to Secure Cyberspace. February 2003. URL: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

9. Cyber Resilience. Playbook for PublicPrivate Collaboration. URL: http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf

10. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с.

11. Carr M. Public-private partnerships in national cyber-security strategies. International Affairs. 2016. № 92(1). P. 43-62; Bures O. Contributions of private business to the provision of security in the EU: beyond public-private partnerships. Crime, Law and Social Change. 2017. № 67(3). P. 289-312.

12. Kim J. Cyber-security in government: reducing the risk. Computer Fraud & Security. 2017. № 2017(7). P. 8-11.

13. Christensen K. K., Petersen K. L. Public-private partnerships on cyber security: a practice of loyalty. International Affairs. 2017. № 93(6). P. 1435-1452.

14. Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 2013. 20 p.

15. Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A192%3AFIN#document1

16. NIS Directive on security of network and information systems. URL: https://ec.europa.eu/digital-single-market/en/news/directive-security-network-and-information-systems-nis-directive

17. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148

18. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

19. Сайт Міністерства розвитку економіки, торгівлі та сільського господарства. URL: http://www.me.gov.ua/Documents/Detail?lang=uk-UA&id=196d3373-eb07-4834-a61e-b3608f28eb22&title=SutnistDerzhavnoprivatnogoPartnerstva

20. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. *Офіційний вісник України*. 2019. № 50. ст. 1697.

21. ІнАУ пропонує кроки до ефективного державно-приватного партнерства в сфері кібербезпеки. https://inau.ua/news/inau-proponuye-kroky-do-efektyvnogo-derzhavno-pryvatnogo-partnerstva-v-sferi-kiberbezpeky.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

УДК 355.402

КРАВЧЕНКО Р.М., *кандидат юридичних наук*

МОЖЛИВОСТІ АДАПТАЦІЇ ІНОЗЕМНОГО ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ТА ОРГАНІЗАЦІЙНОЇ ПОБУДОВИ ОРГАНІВ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ

Анотація. *У статті на підставі проведеного аналізу нормативно-правових актів, що регулюють суспільні відносини в сфері контррозвідувального забезпечення збройних сил країн ЄС, виявлено та виокремлено правові рішення, які можуть бути адаптовані до національного законодавства в інтересах підвищення ефективності здійснення контррозвідувального забезпечення Збройних Сил України, а також правового забезпечення діяльності та організаційної побудови органів військової контррозвідки СБ України. За результатами проведеного дослідження автором запропоновано науково обґрунтовані пропозиції щодо вдосконалення законодавчого підґрунтя діяльності органів військової контррозвідки СБ України.*

Ключові слова: *органи військової контррозвідки, правове забезпечення, організаційна побудова, іноземний досвід.*

Summary. *Ukraine's course on European integration requires an active search for effective mechanisms of participation in the construction of modern European security architecture. Based on the analysis of legislative acts in the field of counterintelligence support of the armed forces of the EU States, the author has identified legal solutions that can be adapted into national legislation in order to increase the effectiveness of counter-intelligence support of the Armed Forces of Ukraine by the military counter-intelligence bodies of the Security Service of Ukraine, as well as improvements in legislative support for the activities and organizational construction of military counter-intelligence bodies of the Security Service of Ukraine. Here it is presented scientifically based research proposals, which are essential for improving the legislative basis of the activities of military counterintelligence bodies on counterintelligence support of military formations of Ukraine.*

Keywords: *military counterintelligence, counterintelligence support, activity, legal support, organizational construction, adaptation of the European experience*

Аннотация. *Взятый Украиной курс на евроинтеграцию требует активного поиска эффективных механизмов участия в строительстве современной архитектуры европейской безопасности. В этой связи в статье на основании проведенного анализа нормативно-правовых актов, регулирующих общественные отношения в сфере контрразведывательного обеспечения вооруженных сил государств ЕС, автором выявлены правовые решения, которые могут быть адаптированы в национальное законодательство в интересах повышения эффективности контрразведывательного обеспечения вооруженных Сил Украины органами военной контрразведки СБ Украины, а также усовершенствования законодательного обеспечения деятельности и организационного построения органов военной контрразведки СБ Украины. По результатам проведенного исследования изложены научно обоснованные предложения, которые имеют существенное значение для усовершенствования законодательной основы деятельности органов военной контрразведки по контрразведывательному обеспечению воинских формирований Украины.*

Ключевые слова: *военная контрразведка, контрразведывательное обеспечение, деятельность, правовое обеспечение, организационное построение, адаптация европейского опыта.*

Постановка проблеми. Сучасні глобалізаційні тенденції та процеси здійснюють безпосередній вплив на стан державної безпеки України, зокрема на збереження її

конституційного ладу, територіальної цілісності й недоторканності [1]. Водночас стратегічний курс України на євроінтеграцію вимагає активного пошуку ефективних механізмів та інструментів участі у побудові сучасної архітектури європейської безпеки. Він передбачає не тільки оперативну сумісність основних складових вітчизняного сектору безпеки і оборони з відповідними структурами європейських країн, але й проведення продуманого реформування основних елементів, що забезпечують національну безпеку в загальному контексті світових тенденцій [2].

На сьогодні в Україні стоїть питання щодо реформування Служби безпеки України, головною метою якого є утворення ефективної, динамічної та гнучкої в управлінні спеціальної служби, укомплектованої високопрофесійними фахівцями, приведення завдань, функцій і напрямів її діяльності у відповідність з актуальними потребами захисту суспільства та держави від зовнішніх та внутрішніх загроз. Одним із напрямів реформування власних спеціальних служб є вивчення досвіду іноземних держав, зокрема окремих країн ЄС [3].

Вирішення завдань підвищення ефективності контррозвідувального забезпечення Збройних Сил України вимагає вивчення можливостей адаптації іноземного досвіду правового забезпечення діяльності та організаційної побудови органів військової контррозвідки.

Результати аналізу наукових публікацій. Проблеми законодавчої регламентації контррозвідувальної діяльності та її напрямів стали предметом вивчення І. Авдошина, О. Довганя, А. Марущака, Г. Новицького, В. Пилипчука, М. Романова, І. Слюсарчука, М. Стрельбицького, Р. Чорного, М. Шиліна, В. Ярковського та інших. Питання врахування практики окремих країн, вихідні умови розвитку та комплекс загроз яких наближені до тих, що характерні для України, опрацьовували С. Фальченко та В. Гребенюк. Незважаючи на достатньо широке коло наукових доробок стосовно проблем адаптації в національне законодавство іноземного досвіду правового забезпечення діяльності та організаційної побудови внутрішніх служб безпеки, проблеми, пов’язані з упровадженням кращих зразків правового регулювання на сучасному етапі діяльності органів військової контррозвідки, залишаються ще недостатньо опрацьованими.

Метою статті є визначення існуючих в законодавстві іноземних держав елементів правового статусу органів військової контррозвідки, які доцільно враховувати при формуванні підходів до удосконалення законодавчих та організаційно-правових засад контррозвідувального забезпечення Збройних Сил України.

Виклад основного матеріалу. Проведений аналіз організаційних основ діяльності органів військової контррозвідки в іноземних країнах [4], національних законодавств, що регулюють їх правовий статус [5], європейських принципів права в розподілі повноважень спеціальних служб щодо контррозвідувального забезпечення військових формувань [6], дозволив автору сформулювати пропозиції з адаптації іноземного досвіду правового забезпечення та організаційної побудови органів військової контррозвідки СБУ (ВКР СБУ). Так, підвищенню ефективності діяльності органів ВКР СБУ, на нашу думку, могло б сприяти розширення законного підґрунтя діяльності за рахунок юридичного закріплення наступних елементів правового положення.

1. Визначення системи органів військової контррозвідки, включаючи центральний орган управління, територіальні підрозділи та їх структуру.

2. Встановлення граничної чисельності особового складу органів військової контррозвідки у відсотковому відношенні до загальної чисельності збройних сил та інших військових формувань.

3. Нормативне визначення завдань та повноважень органів військової контррозвідки, що охоплюються поняттям контррозвідувальне забезпечення збройних сил.

4. Заборона покладання на органи військової контррозвідки завдань, не пов'язаних із забезпеченням державної безпеки.

5. Нормативне визначення необхідності розробки річної програми контррозвідувального забезпечення збройних сил, яка повинна містити, серед іншого, завдання, які необхідно виконати; обсяг і послідовність реалізації цих завдань; пріоритети роботи; критерії виконання/невиконання визначених завдань і пріоритетів, а також порядок її затвердження та звітування за результатами виконання.

6. Визначення завдання інформаційно-аналітичної діяльності органів військової контррозвідки, як проведення заходів щодо встановлення системних причин та передумов виникнення загроз збройним силам, протидію яким віднесено до компетенції органів військової контррозвідки. Встановлення, що інформаційно-аналітична діяльність повинна здійснюватися органами військової контррозвідки виключно для реалізації своїх повноважень.

7. Правова регламентація діяльності органів військової контррозвідки в сфері протидії кіберзагрозам збройним силам.

8. Визначення завдань органів військової контррозвідки в системі інформаційної боротьби, як системи скоординованих заходів інформаційно-психологічного та інформаційно-технічного характеру, які проводяться з метою створення сприятливих умов для успішного ведення воєнних дій, а також захисту власного інформаційного середовища.

9. Законодавче закріплення завдання органів військової контррозвідки щодо контррозвідувального забезпечення миротворчих контингентів збройних сил.

10. Нормативне визначення повноважень органів військової контррозвідки по відношенню до суб'єктів господарювання, які виконують роботи чи надають послуги оборонного призначення, в тому числі пов'язані з перебуванням на військових об'єктах та отриманням доступу до державної таємниці. Включення відповідних вимог, що стосуються забезпечення контррозвідувального режиму, в положення договорів, які укладає оборонне відомство.

11. Визначення категорій осіб (таких як військовослужбовці та працівники збройних сил, члени їх сімей, працівники підрядних організацій Міністерства оборони, колишні військовослужбовці, якщо питання стосуються періоду проходження ними військової служби), у відношенні яких органами військової контррозвідки можуть проводитися відповідні контррозвідувальні заходи.

12. Правова фіксація можливостей органів військової контррозвідки проводити у збройних силах колективні та індивідуальні інструктивні заняття з метою доведення до військовослужбовців, працівників та співробітників підрядних організацій, що виконують оборонні замовлення, інформації про юридичні аспекти кримінального покарання за шпигунство та інші злочини проти національної безпеки, відомостей у визначеному обсязі стосовно іноземних розвідувальних служб, цілей та видів їхньої діяльності, методів проведення розвідувальних операцій, ознак проведення розвідувально-підривної діяльності, залучення до конфіденційного співробітництва, способів підтримання зв'язку, фінансування, міжнародного тероризму та споріднених загроз безпеці особового складу, майну збройних сил та інформації військового характеру, превентивних заходів, які доцільно вживати особовому складу збройних сил та членам їх сімей;

13. Запровадження норми права щодо обов'язкового щорічного проходження кожним військовослужбовцем та працівником збройних сил групових чи індивідуальних

занять контррозвідувальної спрямованості. При цьому, індивідуальні інструктивні заняття повинні проводитися з певними категоріями військовослужбовців (тими, що мають доступ до особливо важливої таємної інформації, криптографічних даних, науково-технічної діяльності оборонної спрямованості, розвідувальної діяльності, підтримують обумовлені службовою необхідністю контакти з іноземними науковцями, студентами, офіцерами зв'язку, планують виїхати до визначених країн, взяти участь у міжнародних науково-технічних заходах, навчаннях, тренуваннях, версифікаційній діяльності, виконувати обов'язки військових аташе за кордоном, народилися, мешкали чи мають родичів у визначених країнах).

14. Нормативне закріплення обов'язків військовослужбовців та працівників збройних сил, виконання яких є необхідним для реалізації органами військової контррозвідки своїх функцій:

- вживати заходи, або утримуватись від певних дій, в інтересах запобігання негативному впливу розвідувально-підривної діяльності іноземних спецслужб;

- проходити щорічні тренування (заняття/інструктажі) з метою доведення органами військової контррозвідки інформації щодо загроз іноземної розвідувальної, терористичної діяльності, а також кіберзагроз комп'ютерним мережам та автоматизованим системам;

- повідомляти встановленим порядком органам військової контррозвідки визначену інформацію щодо фактів або ознак, розвідувальної, терористичної, антиконституційної, іншої підривної діяльності, в тому числі пов'язаної з несанкціонованим доступом до автоматизованих систем і комп'ютерних мереж, у відношенні власних або відомих контактів з особами, які можуть бути причетними до іноземних спецслужб та терористичних організацій.

15. Встановлення дисциплінарної відповідальності військовослужбовців та працівників збройних сил за невиконання обов'язку щодо надання до органів військової контррозвідки інформації про факти чи ознаки розвідувально-підривної діяльності.

16. Впровадження в систему військової освіти та бойової підготовки у збройних силах тренувальних курсів щодо ознак розвідувально-підривної діяльності у відношенні збройних сил та порядку повідомлення про них органів військової контррозвідки. Вказані курси повинні розроблятися органами військової контррозвідки і можуть бути поєднані з інформаційними програмами щодо забезпечення безпеки функціонування автоматизованих систем, охорони державної таємниці та службової інформації.

17. Надання органам військової контррозвідки права, в окремих випадках, для виконання своїх завдань тимчасово залучати військовослужбовців збройних сил.

18. Встановлення обов'язку військового командування та органів військового управління збройних сил, військовослужбовцям сприяти органам військової контррозвідки у виконанні ними своїх завдань, а також їх права вимагати від військовослужбовців припинення дій, що перешкоджають здійсненню завдань і функцій органів військової контррозвідки.

19. Правова регламентація взаємних прав та обов'язків співробітників військової контррозвідки та командирів відповідних рівнів, зокрема в частині інформування військових посадових осіб у визначеному обсязі щодо запланованої чи поточної контррозвідувальної діяльності, яка проводиться у певному операційному районі чи в сфері відповідальності цього командування.

20. Запровадження адміністративної відповідальності військовослужбовців та працівників збройних сил за невиконання законних вимог посадових осіб органів військової контррозвідки.

21. Створення юридичних підстав участі співробітників військової контррозвідки у службових розслідуваннях, що проводяться у збройних силах за фактами зникнення або дезертирства військовослужбовців та працівників, які протягом останнього року мали доступ до цілком таємної чи службової інформації в сфері оборони, перебували в підрозділах спеціального призначення; порушення вимог режиму секретності; несанкціонованого доступу до електронно-обчислювальних машин та автоматизованих систем передачі інформації; вчинення чи спроб вчинення самогубства військовослужбовцями та працівниками збройних сил, які мали доступ до таємної чи службової інформації.

22. Нормативне закріплення можливостей отримання контррозвідувальної інформації шляхом допитів полонених та перебіжчиків, вивчення захоплених у противника документів, зразків озброєння і техніки.

23. Запровадження правових підстав для проведення органами військової контррозвідки інструментальних психофізіологічних досліджень із застосуванням поліграфу, зокрема, у зв'язку з наданням військовослужбовцям збройних сил допуску до інформації з обмеженим доступом чи залученням до робіт, призначенням до розвідувальних підрозділів, доступом до шифрувальних документів та приміщень.

24. Встановлення підстав та порядку доступу органів військової контррозвідки до баз даних збройних сил, у тому числі автоматизованих інформаційних і довідкових систем, реєстрів та банків даних.

25. Надання органам військової контррозвідки права вносити у межах своєї компетенції військовому командуванню подання щодо усунення порушень, причин і умов, що сприяють проведенню розвідувально-підривної діяльності.

26. Надання органам військової контррозвідки права створювати власні бази даних, необхідні для забезпечення щоденної діяльності у сфері контррозвідувальної діяльності, трудових, фінансових, управлінських відносин, відносин документообігу.

27. Створення правових підстав для забезпечення органів військової контррозвідки охороною, транспортом та засобами зв'язку (у тому числі спеціальними), засобами індивідуального захисту, вогнепальною зброєю, іншим необхідним майном, обмундируванням, приміщеннями в межах відповідних військових гарнізонів за рахунок збройних сил.

28. Запровадження кримінальної відповідальності за саботаж, як навмисне невиконання військовослужбовцями своїх обов'язків, чи навмисне недбале їх виконання зі спеціальною метою завдання шкоди бойовій готовності збройних сил. Визначення обов'язком органів військової контррозвідки здійснювати у збройних силах виявлення, попередження та припинення саботажу, який здійснюється за завданням іноземних спецслужб та організацій.

29. Визначення місця та завдань співробітників військової контррозвідки в похідному порядку при пересуванні підрозділів збройних сил на марші, а також при розміщенні підрозділів у призначеному районі розташування.

30. Визначення заходів контррозвідувальної підтримки військ на етапах підготовки до бою, ведення бою та виходу з бою, їх включення до бойових наказів, планів проведення бойових операцій, замислів виконання тактичних бойових завдань.

31. Введення статутної норми, згідно з якою командирам відповідних рівнів при виданні бойових наказів чи складанні планів проведення бойової операції рекомендовано визначати заходи контррозвідувальної підтримки військ на етапах підготовки до бою, ведення бою та виходу з бою, а також інтегрувати заходи контррозвідувальної підтримки до всіх планів, тренувань, систем, занять, доктрин, та стратегій.

При цьому необхідно сказати, що Україна в цілому потребує подальшої розбудови системи правового гарантування національної безпеки шляхом напрацювання відповідних законів, концепцій, доктрин, стратегій і програм. З огляду на це актуальною постає проблема розвитку правової науки в галузі національної безпеки та інституційного забезпечення її становлення [7].

Висновки.

Таким чином, упровадження іноземного досвіду, зокрема щодо вищерозглянутих норм, у законодавство України, дасть змогу підвищити ефективність контррозвідувального забезпечення військових формувань України та удосконалить законодавче підґрунтя діяльності та організаційної побудови військової контррозвідки Служби безпеки України.

Результати проведеного дослідження доцільно використати в ході розробки пропозицій з удосконалення законодавчих та організаційно-правових засад контррозвідувального забезпечення Збройних Сил України.

Використана література

1. Пилипчук В.Г., Дзьобань О.П. Вплив глобалізаційних процесів на конституційний лад, територіальну цілісність і недоторканність України. *Гуманітарний часопис*. 2010. № 1. С. 5-10. URL: http://nbuv.gov.ua/UJRN/gumc_2010_1_3

2. Єрмолаєв Д.І. Реформування розвідувальних, контррозвідувальних та спеціальних служб після холодної війни: світовий досвід. *Інвестиції: практика і досвід*. 2013. № 23. С. 139-142. URL: http://nbuv.gov.ua/UJRN/ipd_2013_23_32

3. Ходанович В.О. Окремі питання виявлення й розслідування шпигунства в Україні та ФРН. *Науковий вісник міжнародного гуманітарного університету. Серія: Юриспруденція*. 2018. Вип. 31. С. 130-133. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2018_31_35

4. Кравченко Р.М. Організаційні основи діяльності органів військової контррозвідки в європейських країнах. *Вісник Академії адвокатури України*. 2018. № 1–2. С. 151-160.

5. Кравченко Р.М. Функціональні моделі органів військової контррозвідки в державах Європи: збірник матеріалів Міжнародної науково-практичної конференції *Виклики політики безпеки,* м. Львів, 15 жовтня 2018 року. Львів, 2018. С. 132-134.

6. Кравченко Р.М. Роль європейських принципів права у визначенні повноважень органів військової контррозвідки Служби безпеки України щодо контррозвідувального забезпечення військових формувань. *Інформаційна безпека людини, суспільства, держави*. 2019. № 1(25). С.74-84.

7. Пилипчук В. Пріоритети розвитку права і правової науки в галузі безпеки в умовах глобалізації та геополітичних трансформацій. *Вісник Академії правових наук України*. 2009. № 3. С. 3-13. URL: http://nbuv.gov.ua/UJRN/vapny_2009_3_1

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~
~~~~~~~~~~~~~~

Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"

УДК 61:316.422

БЕЛАНЮК М.В., *кандидат юридичних наук,* учений секретар
НДІ інформатики і права НАПрН України
РАДЗІЄВСЬКА О.Г., *кандидат юридичних наук*, провідний науковий співробітник
НДІ інформатики і права НАПрН України
МАНЬГОРА Т.В., *кандидат юридичних наук*, старший викладач
Вінницького Національного аграрного університету

ТРАНСФОРМАЦІЯ СИСТЕМИ ОХОРОНИ ЗДОРОВ'Я В УКРАЇНІ

Анотація. *В Україні з 2017 року триває реформа системи охорони здоров'я, яка передбачає проведення комплексу заходів та змін з метою трансформації цієї системи у більш прогресивну модель, задля покращення життя і здоров'я громадян. У статті висвітлено проблемні питання реформування окремих елементів системи охорони здоров'я в Україні. З урахуванням думок фахівців та вчених галузі виявлено ряд проблем, які можуть виникнути при реалізації запроваджених урядом змін та запропоновано шляхи їх подолання.*

Ключові слова: *реформа охорони здоров'я, медична галузь, медицина.*

Summary. *Since 2017, a reform of the healthcare system has been ongoing in Ukraine, which envisages a series of measures and changes in order to transform it into a more progressive model in order to improve the life and health of citizens. The article highlights the problematic issues of reforming certain elements of the healthcare system in Ukraine. Taking into account the opinions of experts and scientists of the industry, a number of problems that may arise in implementing the changes introduced by the government have been identified and ways to overcome them have been proposed.*

Keywords: *healthcare system reform, healthcare industry, medicine.*

Аннотация. *В Украине с 2017 года идет реформа системы здравоохранения, которая предусматривает проведение комплекса мероприятий и изменений с целью трансформации этой системы в более прогрессивную модель для улучшения жизни и здоровья граждан. В статье освещены проблемные вопросы реформирования отдельных элементов системы здравоохранения в Украине. Учитывая мнения специалистов и ученых медицинской сферы выявлено ряд проблем, которые могуть возникнуть во время реализации введенных правительством изменений и предложены пути их решения.*

Ключевые слова: *реформа здравоохранения, отрасль медицины, медицина*.

Постановка проблеми. Найвищою соціальною цінністю у світі визнаються життя і здоров'я людини. Право на здоров'я – це одне з основних прав людини. У статті 49 Конституції України закріплено кожному громадянину право на охорону здоров'я, медичну допомогу та медичне страхування, а держава має створювати відповідні умови для ефективного і доступного медичного обслуговування [1].

За оцінкою Європейського регіонального бюро Всесвітньої організації охорони здоров'я (ВООЗ), сучасний стан здоров'я української нації характеризується низьким рівнем тривалості життя, вкрай високими показниками захворюваності та смертності, відсутністю можливості отримувати доступну медичну допомогу [2].

Незважаючи на те, що Україна витрачає значну кількість свого бюджету на медицину, на сьогодні в Україні склалася ситуація, коли громадяни у разі хвороби мають самостійно оплачувати своє лікування (ліки; вартісне обстеження; утримання в лікарнях у вигляді благодійних внесків тощо), при цьому громадянами покривається 99 % витрат на придбання ліків (у більшості європейських країн ці затрати становлять 30 – 60 %) [3, с. 84-88]. Основними причинами такого стану є суттєві недоліки, національної системи охорони здоров'я: відсутність модернізації, нівелювання потреб населення і сучасних міжнародних тенденцій у зазначеній сфері, економічної неефективності та високого рівня корупції в Україні.

Проведене Київським міжнародним інститутом соціології у березні 2019 року соціологічне дослідження стосовно думок населення щодо якості медичних послуг та проведення реформ охорони здоров'я в Україні за останні 2 роки показало, що 81 % населення вважають необхідним проведення реформ охорони здоров'я [4].

В Україні з 2017 року розпочалась реформа системи охорони здоров'я, яка передбачає проведення комплексу заходів та змін з метою трансформації цієї системи у більш прогресивну модель, яка має на меті покращення життя і здоров'я громадян. Під час наукового пошуку були проаналізовані праці дослідників, які займались вивченням окремих аспектів та проблем реформування системи охорони здоров'я в Україні та світі: Н. Авраменко, О. Дорошенко, К. Вишньовська, Л. Денісова, В. Лехан, Г. Слабкий, М. Шевченко, Б. Розенблат, В. Лазоришинець, І. Трахтенберг та інші [5]. При опрацюванні матеріалів авторами також було враховано думки фахівців галузі та населення України.

Спробуємо дослідити та проаналізувати ефективність трансформації окремих елементів української системи охорони здоров'я з урахуванням проведених урядом заходів. У статті розглянуто лише окремі аспекти реформування системи охорони здоров'я в Україні з огляду на те, що сфера охорони здоров'я складається з численних елементів та потребує поєднання наукових пошуків фахівців різних сфер діяльності.

Метою статті є визначення стану та перспектив окремих елементів системи охорони здоров'я в сучасній Україні на підставі світового досвіду.

Виклад основного матеріалу. У світі відомі моделі систем охорони здоров'я: монопольно-державна або бюджетна (модель Н.А. Семашко (діяла в СРСР); державна або національна (модель У. Беверіджа); страхова медицина (модель О. Бісмарка); ринкова (приватна) модель.

Система охорони здоров'я, побудована ***за моделлю Семашка***, фінансувалась виключно з державного бюджету, базувалася на загальних податках, контролювалася державою через систему централізованого планування та характеризувалася відсутністю приватного сектора.

Перевагами цієї моделі є єдність принципів організації; централізація системи охорони здоров'я; рівна доступність охорони здоров'я для всіх громадян; першочергова увага дитинству та материнству; єдність профілактики і лікування; ліквідація соціальних основ хвороб; залучення громадськості до справи охорони здоров'я тощо.

Недоліками моделі Семашка є бюрократичні та адміністративно-командні методи управління охороною здоров'я та відсутність економічних важелів управління.

У Британії, Данії, Ірландії, Іспанії, Італії, Португалії, Греції, Швеції та колишніх країнах соцтабору запроваджено Державну (національну) систему охорони здоров'я за ***моделлю Беверіджа***.

Для цієї моделі характерно, що основна частина медичних установ належить державі, управління здійснюється центральними та місцевими органами влади,

фінансується з загальних податкових надходжень до держбюджету і охоплює всі категорії громадян. Управління системою здійснюється професійними працівниками, контроль якості – державою і професійними медичними працівниками. Поряд з економним використанням ресурсів (держава стримує зростання витрат на охорону здоров'я за допомогою макроекономічних методів (певний % і не більше). Характерно для цієї моделі нерівність в доступності медичної допомоги для окремих соціальних груп або адміністративних територій.

Недоліки системи Бевериджа: низька оплата праці медперсоналу, через що у лікарів та медичного персоналу немає стимулу для підвищення ефективності лікування; обмеження свободи вибору для пацієнтів, позиція фахівців по центральному плануванню обмежує новаторство, недостатньо враховує місцеві особливості та інтереси; пріоритетне фінансування і використання закладів вторинної допомоги; слабкі зв'язки між центром і периферією, авторитарна система управління. Істотним недоліком також є черги.

Модель Бісмарка заснована на страхуванні здоров'я громадян, запроваджена в Німеччині, Бельгії, Нідерландах, Люксембурзі, Австрії, Швейцарії, Франції, Японії, Канаді та ін. Принцип страхування з більшою чи меншою участю уряду у фінансуванні страхових фондів системи охорони здоров'я в цих країнах є громадським, оскільки управляються органами влади, але на відміну від державних фінансуються за допомогою цільових внесків підприємців, особистих вкладів працюючих, а також бюджетних субсидій.

Основні характеристики системи Бісмарка: децентралізована система, свобода вибору страхових фондів для споживачів і підприємців. Існує конкуренція між страховими компаніями, які приділяють дуже велику увагу контролю якості медичної допомоги і контролю за витратами. Широкий вибір місць лікування.

Основними недоліками системи Бісмарка є: відсутність рівної доступності медичної допомоги для різних категорій громадян і адміністративних територій; зростання вартості медичних послуг; недостатній контроль за діяльністю персоналу; нехтування інтересами пацієнтів, які належать до груп високого ризику (які тривалий час перебувають в стаціонарах, або хворих, які опинилися поза системою страхування); високі адміністративні витрати; низькі пріоритети соціальної системи охорони здоров'я, санітарної освіти, зміцнення здоров'я, нехтування профілактичною медициною.

Ринкова система охорони здоров'я характеризується широким вибором медичних послуг; відсутністю черг; гарантією доступності спеціалізованої медичної допомоги; гарантією конфіденційності лікування, уваги до пацієнта; високою якістю умов госпіталізації тощо.

Недоліками ринкової системи охорони здоров'я є висока вартість медичної допомоги; недоступність для бідних; судові процеси як інструмент контролю якості медичного обслуговування; неадекватний потребам населення розподіл служб охорони здоров'я і відсутність механізму впливу на нього; недостатня профілактика захворювань; низька ступінь використання капіталу і кадрових ресурсів, регулювання і контроль якості лікування.

В сучасному світі не існує жодної країни, яка б мала усталену модель системи охорони здоров'я. Зокрема Італія, Португалія від страхової медицини перейшли до національної бевериджської системи; США, Корея, Кіпр, Ізраїль, Нідерланди – від добровільного страхування до національного загального НМС (так звана "соціалізація"); Росія та країни Центральної та Східної Європи – від державної до системи медичного страхування; Великобританія, Німеччина, Франція, Бельгія, країни Північної Європи,

Канада, Австрія зберегли свої системи з відповідними корективами, ввели загальнообов'язкове медичне страхування на державному рівні. При побудові власних систем охорони здоров'я країни враховували при цьому необхідність забезпечення рівності для всіх громадян та доступності обсягу послуг при досить високій якості.

Відповідно до Розпорядження Кабінету Міністрів України "Про схвалення Концепції реформи фінансування системи охорони здоров'я" від 30.11.16 р. № 1013-р [6] в Україні заплановано проведення зазначеної реформи у три етапи, а саме:

На першому (підготовчому) етапі (2017 рік) передбачено: створення законодавчої бази для функціонування нової системи фінансування охорони здоров'я; утворення єдиного національного замовника медичних послуг; розробка моделі державного гарантованого пакета медичної допомоги; проведення реорганізації закладів охорони здоров'я (створення державних та комунальних некомерційних підприємств; запровадження національної системи реімбурсації лікарських засобів; створення уніфікованих клінічних протоколів; створення необхідних електронних реєстрів (пацієнтів, постачальників та медичних станів).

На другому етапі (2018 – 2019 рр.) передбачено: розробку та прийняття нормативно-правових актів для запровадження державного гарантованого пакета медичної допомоги, механізмів співоплати за медичні послуги, залучення добровільного медичного страхування; початок фінансування державного гарантованого пакета медичної допомоги через єдиного національного замовника медичних послуг; запровадження системи реімбурсації лікарських засобів; затвердження клінічних протоколів для найбільш поширених медичних станів; розробка системи тарифікації медичних послуг; створення госпітальних округів; початок оплати постачальникам медичних послуг, що надають стаціонарну вторинну (спеціалізовану) та третинну (високоспеціалізовану) медичну допомогу за принципом оплати за пролікований випадок.

На третьому етапі (2020 рік) передбачено: фінансування в повному обсязі постачальників медичних послуг, з якими укладено договори з єдиним національним замовником медичних послуг; забезпечення функціонування електронної системи охорони здоров'я; введення повноцінного механізму співоплати за медичні послуги; забезпечення використання нових механізмів оплати медичних послуг, а саме: для первинної медичної допомоги – механізму оплати на основі капітаційної ставки на одного громадянина; для вторинної (спеціалізованої) та третинної (високоспеціалізованої) медичної допомоги – механізму оплати за пролікований випадок; проведення оцінки впровадження нової моделі фінансування системи охорони здоров'я та підготовка плану розвитку системи на наступні п'ять років.

Медична реформа стартувала у 2017 році із затвердження Плану заходів з реалізації Концепції реформи фінансування системи охорони здоров'я на період до 2020 року [7] та прийняттям законів: "Про державні фінансові гарантії надання медичних послуг та лікарських засобів" [8], "Про внесення змін до Бюджетного кодексу України щодо видатків на первинну медичну допомогу" [9], Зміни до Основ законодавства України про охорону здоров'я (до статей 3, 8 та 35) [10] та інші.

Як бачимо, реформування системи охорони здоров'я в Україні пов'язане насамперед із вирішенням завдань його ресурсного забезпечення, а зазначені нормативно-правові акти спрямовані на скорочення витрат державного бюджету на галузь та в основному стосуються питань фінансування системи охорони здоров'я.

На наш погляд здійснити реформу найбільш корумпованої галузі в країні за чотири, та навіть п'ять років неможливо. Наприклад в Туреччині, у країні, яка

випереджає ЄС як за низьким рівнем дитячої смертності, так і за термінами очікування обстеження, а 90 – 95 % населення задоволені медичним обслуговуванням, на впровадження медичної реформи пішло десять років [11]. Однією з передових країн світу за якістю медицини є Німеччина. Однак, друге місце серед тих, хто їде лікуватись до Туреччини, займають саме громадяни Німеччини. Їх влаштовує в Туреччині якісне лікування, швидкість надання медичної допомоги та помірні ціни, включаючи трансплантацію.

В рамках реформи системи охорони здоров'я 27 грудня 2017 р. створено Національну службу здоров'я України (далі – НСЗУ) – замовника медичних послуг та лікарських засобів за програмою медичних гарантій [12]. Отримати безкоштовну медичну послугу пересічний громадянин зможе лише у закладах, які підписали договори та сертифіковані НСЗУ. Сертифікат отримають лише ті заклади, а також обладнання, яке відповідає вимогам Національної служби. Існують й певні обмеження щодо укладання договорів: "договори укладаються лише в межах бюджетних коштів, передбачених на охорону здоров'я на відповідний бюджетний період, на підставі вартості й обсягу послуг з медичного обслуговування". Можна спрогнозувати, що в умовах дефіциту коштів обсяги гарантованої медичної допомоги буде скорочено до меж бюджету. Якщо з точки зору економії – це раціональний і логічний підхід, то з позицій медицини – істотний ризик. Оскільки з урахуванням неможливості точного прогнозу перебігу хвороби пацієнта, його одужання тощо, запровадження механізмів нормованого розподілу витрат і нормування медичних втручань приховує небезпеку невизначеності. Навіть жорстке запровадження протоколів лікування і нормативне фінансування на їх підставі можуть значно обмежити здатність лікаря приймати гнучкі рішення щодо лікування пацієнта і перетворять його з логічномислячого фахівця на суто технічного виконавця [13].

Великою проблемою є отримання сертифікату медичними закладами невеликих містечок чи навіть районних центрів, де застаріле обладнання та апаратура. Наразі такі медустанови фінансуються по-старому (отримують від держави субвенції). Перейти до нової системи фінансування ці заклади не зможуть, поки за рахунок місцевих бюджетів не будуть усунуті всі недоліки (ремонт та устаткування, необхідне обладнання тощо). До цього часу місцева влада зобов'язана поінформувати населення про медзаклади, які отримали сертифікати і там є можливість отримати безкоштовну медичну послугу. На жаль, ми не знайшли такої інформації на офіційних сайтах міст та областей України, хоча така інформація повинна бути відкритою та доступною пересічному громадянину.

За даними соціологічного дослідження, проведеного Київським міжнародним інститутом соціології у березні 2019 року про те, що в Україні створена Національна Служба здоров'я знають лише 21 % українців, 85 % вважають, що якість медичного обслуговування в Україні далека від європейських стандартів. Серед країн, які вони обрали б для лікування: Ізраїль (39 %), Німеччину (38 %), Швейцарію (21 %), США (10 %), Білорусь (8 %), Росію (3 %) [4].

З 2 квітня 2018 року триває обрання громадянами України сімейних лікарів з числа терапевтів та педіатрів, з якими вже підписали договір 78 % населення. Підписання декларації з конкретним лікарем надає можливість пацієнту отримати безкоштовну медичну допомогу, кошти на це виділяє Національна служба здоров'я. Зокрема система працює так: людина заздалегідь записується на прийом до сімейного лікаря через особистий кабінет на сайті "Helsi" або будь-яким іншим доступним способом (наприклад по телефону). Сімейний лікар проводить огляд та видає направлення до вузького спеціаліста, послугу якого оплачує безпосередньо НСЗУ за програмою "гроші йдуть за

пацієнтом”. Втім, є нюанси. Без направлення сімейного лікаря людина не зможе отримувати безкоштовне обслуговування у вузького спеціаліста. Також існує загальна проблема з обрання сімейного лікаря у сільських місцевостях та невеликих містах. Зазвичай в українських селах працює один лікар. Максимальна кількість пацієнтів, з якими він по закону має підписати декларацію – 2000 осіб. Що робити іншим мешканцям? Їхати в район за 50 км. від дому у пошуках сімейного лікаря? А як бути інвалідам, людям які не можуть самостійно пересуватись та ще й пенсії отримують мінімальні, через що неспроможні оплатити навіть поїздку до районної лікарні? Навіть якщо вони й знайдуть лікаря й підпишуть з ним декларацію, чи зможуть вони при потребі відвідувати лікаря, який знаходиться на значній відстані? Ще більш ускладнює ситуацію те, що тепер виїзд лікаря за викликом пацієнта скасовано. Ці питання залишаються без відповіді. Чи буде ефективна модель сімейної медицини в Україні покаже час.

Поряд з цим фахівці вітчизняної медичної галузі переконані у тому, що сімейний лікар – це окрема спеціальність, якої слід навчати, починаючи з вищого навчального закладу. Не можна перевчити лікаря-спеціаліста на сімейного лікаря. Наприклад гастроентеролог з двадцятирічним стажем роботи в дорослій поліклініці не зможе розпізнати раптову екзантему у немовляти, не розпізнає апоплексію яєчника, пропустить менінгіт і не запідозрить туберкульоз лімфовузлів. А введення штрафів за звертання сімейного лікаря за консультацією до спеціаліста – нісенітниця [14].

Іншою загальною проблемою сімейної медицини, як в країнах Західної Європи, так і в США, є те, що пацієнтам досить складно отримати направлення сімейного лікаря до спеціаліста, хіба що хвороба наскільки є небезпечною, що лікар, побоюючись відповідальності за життя пацієнта, вимушений все ж направити його до спеціаліста. Зазвичай сімейні лікарі неохоче направляють хворих до вузьких спеціалістів, оскільки не хочуть оплачувати консультацію, очікуючи поки пацієнт звернеться за платною допомогою. Навіть якщо пацієнт і отримає направлення до вузького спеціаліста, має чекати своєї черги від двох тижнів до двох місяців.

В Україні на сьогодні такої проблеми немає. Потрапити від сімейного лікаря до спеціаліста можна за один-два робочих дні. Чи потрібно Україні копіювати складні шляхи для отримання медичної допомоги на другому та третьому рівні, що в свою чергу обов’язково призведе до емоційної напруги у суспільстві та позначиться на здоров’ї громадян? На нашу думку, не слід вводити повну заборону самозвернень пацієнтів до спеціалістів. Створення збалансованої системи первинної медико-санітарної допомоги потребуватиме часу для напрацювання певного досвіду.

Основним принципом медичної реформи в Україні визначено принцип “гроші ходять за пацієнтом”. Офіційного штатного розкладу лікувальні заклади не матимуть. Головний лікар має на власний розсуд визначити необхідну кількість медперсоналу лікувальної установи. При прибутті пацієнта на обстеження та лікування мають прийти в лікарню гроші від Національної служби здоров’я згідно з тарифом за надані пацієнтам медичні послуги. Кількість грошей у медзакладі буде залежати від кількості пацієнтів. Отже, щоб заробити більше грошей, медзаклади будуть зацікавлені у великій кількості пацієнтів, щоб всі ліжко-місця постійно були заповненими, а ті заклади, які будуть визнані неефективними будуть або ліквідовані, або приватизовані.

В Україні майже всі державні лікарні потребують великих капітальних вкладень на ремонт і закупівлю необхідного устаткування, через що вони не можуть конкурувати з приватними. Інший аспект: якщо сучасні приватні лікарні можуть спрямовувати кошти, отримані за надання послуг від НСЗ, на оплату праці своїх працівників та покращення якості лікування, то державні медзаклади вимушені будуть спрямовувати ці кошти

насамперед на матеріальне оснащення своїх медзакладів, а потім вже думати про якість послуг та підвищення заробітних плат своїм працівникам. Тобто на початковому етапі реформи системи охорони здоров'я не створено рівних умов між приватним і державним секторами медичної галузі.

Щодо ефективності запровадження національної системи реімбурсації лікарських засобів звернімося до статистики. Соціологічне дослідження (березень 2019 р.) показало, що 60 % українців знають про програму "Доступні ліки", але лише 19 % стверджують, що особисто чи їхні близькі родичі брали в ній участь. Серед осіб віком 60 років і старше лише 27 % беруть участь у програмі [4]. Тобто 81 % населення не користується програмою реімбурсації. Чи може це свідчити про її ефективність?

Інша проблема може виникнути через закупівлю лікарських препаратів за завищеними цінами й низької якості. Нині аптеки завалені ліками виробництва країн третього світу, де може не бути навіть основного компоненту (діючої речовини). Очільники МОЗ Україні стверджують, що ціни на ліки в Україні є завищеними і недостатнє фінансування галузі не дозволяє впровадити реімбурсацію за такими цінами. Тому в якості референтних цін слід орієнтуватись на Польщу, Латвію, Словаччину, Угорщину, Чехію. Кореспонденти газети "Аптека" провели власне дослідження, результати якого свідчать, що середньозважена вартість однієї упаковки лікарського засобу в Україні є однією з найнижчих серед сусідніх та європейських країн. Також за даними аналітичної системи дослідження ринку "PharmXplorer"/"Фармстандарт" компанії "Proxima Research" цей показник у країнах СНД у 2015 р. становив: у Росії – 3,39 дол.; у Казахстані – 3,13 дол.; у Білорусі – 2,48 дол.; у Грузії – 3,77 дол., а в Україні – 2,05 дол. [15].

Експерт з впровадження медичної реформи на місцевому рівні А. Макаріхіна впевнена, що сьогодні не всі лікарні готові до самостійності в рамках переформатування на госпітальні округи (державні медичні заклади, які знаходяться на території районів, об'єднуються та переходять у власність об'єднаних територіальних громад (ОТГ). Для формування госпітальних округів не вистачає кадрів, низький рівень економістів у медичній галузі, є потреба у покращенні навичок персоналу у користуванні комп'ютерною технікою тощо [16].

Дискусійним, на нашу думку, є намір створення, за зразком країн ЄС, лікарень, об'єднаних в госпітальні округи, в яких існуватимуть усі напрямки лікування, натомість ліквідувавши спеціалізовані профільні лікарні України. Але ж найкращу якісну медичну допомогу може надати лікар, який спеціалізується на однотипних операціях, які проводить постійно, ніж багатопрофільні хірурги обласних лікарень, яким доводиться робити різні операції.

Реформування системи охорони здоров'я передбачає застосування міжнародних клінічних протоколів обстеження та лікування захворювань. Слід зауважити, що не існує такого поняття, як міжнародний протокол. Кожна країна має свій науковий, дослідницький, матеріальний потенціал. Тому клінічний протокол – основний медико-технологічний документ, яким мають керуватися медичні фахівці в кожній конкретній клінічній ситуації, уникаючи неефективних та помилкових рішень, може бути лише національним. В Україні функціонує Національна академія медичних наук України (далі – НАМН України), фахівці якої мають бути залучені до розробки національного протоколу обстеження та лікування захворювань. Для порівняння: вартість лікування у закладах НАМН України у 20 разів нижча, ніж в США та у 10 разів нижча за такі країни, як Німеччина та Італія, у 2 – 3 рази нижча ніж в Латвії, Литві і Казахстані [17].

Автономізація НАМН України та переведення її інститутів у статус комунальних некомерційних підприємств, як пропонує Міністерство охорони здоров'я, призведе до згортання медичних досліджень та ліквідації взагалі медичної науки в Україні. Цього робити категорично не можна. Метою комунальних некомерційних підприємств є надання послуг з охорони здоров'я населенню, а метою науки – одержання нових знань та пошук шляхів їх застосування. На сьогодні держава виділяє лише 30 – 40 % від фінансових потреб НАМН України. За словами французького фізика П'єра Кюрі: "Країна, яка не розвиває власну науку, неминуче стає колонією" [18].

В Україні простежується тенденція до скорочення витрат і на медичну науку і на медичну галузь в цілому. Так у 2008 р. загальні витрати на охорону здоров'я складали 6,64 % ВВП, у 2012 р. – 7,7 % ВВП, у 2018 р. – 3,7% ВВП, у 2019 р. – 3,2 % ВВП [18]. За висновками Всесвітньої організації охорони здоров'я, якщо держава виділяє на охорону здоров'я менше, ніж 5 % ВВП, медична галузь неминуче деградує [17].

Висновки.

Дослідження доводить, що швидкими темпами (4 – 5 років) неможливо здійснити якісні реформи медичної галузі. В Україні розпочато реформування системи охорони здоров'я та прийнято ряд заходів, у тому числі й щодо скорочення витрат державного бюджету на забезпечення системи охорони здоров'я, без необхідної підготовчої роботи: дослідження ефективності існуючої системи, вивчення вітчизняного та світового досвіду, необхідних підрахунків із залученням фахівців різних сфер життєдіяльності (вчених, лікарів, економістів та ін.).

В Україні створено Національну службу здоров'я України – замовника медичних послуг та лікарських засобів за програмою медичних гарантій. Запроваджено механізм отримання сертифікатів медичними закладами, але не всі заклади можуть їх отримати через невідповідність вимогам НСЗУ (зокрема державні).

Населення країни недостатньо поінформовано про зміни в системі охорони здоров'я та можливість отримання безкоштовної медичної допомоги. Соцопитування 2019 р. показало, що 85 % населення незадоволено якістю медичного обслуговування в Україні.

Із запровадженням реформи терапевти та педіатри перетворюються на сімейних лікарів, яких не вистачає, особливо у невеликих містечках та селах. Перекваліфікація у сімейних лікарів без необхідної підготовки може призвести до випадків неправильної діагностики хвороби у пацієнтів, що в свою чергу може призвести до погіршення стану здоров'я населення. Шлях за направленням від сімейного лікаря до спеціаліста може значно ускладнити можливість отримання швидкої безплатної медичної допомоги та призвести до фактів корупції.

Принцип "гроші ходять за пацієнтом" може призвести до ліквідації або приватизації державних медичних закладів через їх неконкурентоспроможність із приватними.

Програма реімбурсації лікарських засобів виявилась неефективною, нею користуються лише 20 % населення. Це також може свідчити про недостатню поінформованість населення.

Якість та ціна вітчизняної фармацевтичної продукції можуть певним чином конкурувати з іноземною, а лікувальні протоколи мають бути вітчизняними.

Питання щодо ліквідації спеціалізованих профільних лікарень та створення багатопрофільних медичних установ є дискусійним та потребує додаткового опрацювання та дослідження, оскільки може позначитись на якості надання медичної допомоги.

Мета медичної науки – одержання нових знань та пошук шляхів їх застосування. Автономізація Національної академії медичних наук України призведе до ліквідації медичної науки, що в свою чергу поставить медичну галузь України у залежність від іноземних країн.

Головною метою реформування системи охорони здоров'я України має бути забезпечення населення країни гарантованим правом на максимальний захист свого здоров'я: повноцінною, якісною та доступною медичною допомогою. Реформа має бути спрямована на подолання корупції та запобігання зайвих витрат. Кожна країна здійснює реформи з урахуванням власних національних традицій, світового та національного досвіду, оскільки охорона здоров'я в кожній країні є продуктом історії нації. Реформування охорони здоров'я має бути прагматичним, відштовхуватись від того, що існує, а не мислити абстрактно. Не слід вводити кардинальні зміни одночасно, поступові реформи мають шанс бути більш успішними та уникнути незворотних процесів.

Україна має значний науковий потенціал. Саме вчені мають відповісти на запитання, яка система охорони здоров'я потрібна країні та долучитись до її розробки із залученням фахівців галузей, дотичних до системи охорони здоров'я (пацієнтів, страховиків, медичних працівників, економістів, юристів, органи місцевого самоврядування та ін.), провести необхідні статистичні спостереження та розрахунки: перепис населення (останній був у 2001 р.), дослідити стан матеріально-технічної бази, провести аудит тощо. В Україні існує проблема з медичними кадрами у невеликих містах і селах і цю проблему потрібно вирішувати на державному рівні. На нашу думку в Україні має бути обов'язкова страхова медицина. Слід також забезпечити доступну, достовірну, правдиву, своєчасну і прозору інформацію стосовно охорони здоров'я для всіх громадян.

Світовий досвід доводить, що бюджет охорони здоров'я має становити не менше 5 % ВВП, а в Україні ця цифра щороку зменшується, не зважаючи на пришвидшене реформування галузі, яке прогнозовано потребуватиме додаткових витрат.

З розвитком суспільних процесів, викликаних глобалізацією, інформатизацією та інноватикою галузь охорони здоров'я потребуватиме постійних змін і реформ, тому необхідно застосовувати всебічний і комплексний підхід до реформ.

Використана література

1. Основи законодавства України про охорону здоров'я: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2801-12; Цивільний кодекс України: Закон України. URL: https://zakon.rada.gov.ua/laws/show/435-15; Про екстрену медичну допомогу: Закон України. URL: https://zakon.rada.gov.ua/laws/show/5081-17

2. Про реформу охорони здоров'я в Україні: Рекомендації парламентських слухань від 16 грудня 2015 року. URL: https://zakon.rada.gov.ua/laws/show/1338-viii

3. Загальні витрати на охорону здоров'я в Україні (за даними національних рахунків охорони здоров'я). *Україна. Здоров'я нації: наук.-практ. вид*. – (Укр. ін-т стратег. дослідж. МОЗ України). Київ: Вид-во. "Експерт", 2010. № 2(14). С.84-88.

4. Думки і погляди населення України щодо охорони здоров'я та інших питань, березень 2019. – (Київський міжнародний інститут соціології). URL: http://kiis.com.ua/?lang=eng&cat=reports&id=861&page=1

5. Авраменко Н.В. Механізми фінансування системи охорони здоров'я України. *Теорія та практика державного управління*. 2009. Вип. 2. С. 187-192; Лехан В.М. Слабкий Г.О., Шевченко М.В. Стратегія розвитку системи охорони здоров'я: український вимір. Київ, 2009. 50 с.; Основні шляхи подальшого розвитку системи охорони здоров'я в Україні / під заг. ред. В.М. Лехан, В.М. Рудого. Київ: Вид-во Раєвського, 2005. 168 с.; Lekhan V.N., Rudiy V.M., Shevchenko M.V. Ukraine: Health system review. Health Systems in Transition; World Health

Organization (acting as the host organization for, and secretariat of, the European Observatory on Health Systems and Policies), WHO Regional Office for Europe. Copenhagen, 2015. V. 17(2). 153 p.

6. Про схвалення Концепції реформи фінансування системи охорони здоров'я: Розпорядження КМ України від 30.11.16 р. № 1013-р. URL: https://zakon3.rada.gov.ua/laws/show/1013-2016-%D1%80

7. Про затвердження плану заходів з реалізації Концепції реформи фінансування системи охорони здоров'я на період до 2020 року: Розпорядження КМ України від 15.11.17 р. № 821-р. URL: https://zakon.rada.gov.ua/laws/show/821-2017-%D1%80

8. Про державні фінансові гарантії медичного обслуговування населення: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2168-19

9. Про внесення змін до Бюджетного кодексу України щодо видатків на первинну медичну допомогу: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2233-19

10. Зміни до Основ законодавства України про охорону здоров'я: Закон України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61567

11. Шлапак А. Турецька медицина. – (ALL INCLUSIVE). URL: https://blogs.pravda.com.ua/authors/shlapak/528f72f6d86e0/

12. Про утворення Національної служби здоров'я України: Постанова КМ України від 27.12.17 р. № 1101. URL: https://zakon.rada.gov.ua/laws/show/1101-2017-%D0%BF

13. Дорошенко О.О., Шевченко М.В. Аналіз міжнародного досвіду фінансування вторинної медичної допомоги. *Економіка і право охорони здоров'я*. 2017. № 1(5).

14. Ось-ось полетять у прірву залишки старої медицини – а от чи виживемо ми з новою, велике питання. URL: https://tsn.ua/blogi/themes/health_sport/reformi-abo-mamo-mi-vsi-pomremo-945605.html?utm_source=page&utm_medium=readmore

15. Ціноутворення та реімбурсація: про що говорив Володимир Гройсман із фармацевтичною індустрією? URL: https://www.apteka.ua/article/392193

16. У Запоріжжі обговорили особливості реформи медзакладів вторинного рівня. – (11.09.2019). URL: https://www.ukrinform.ua/rubric-regions/2777851-u-zaporizzi-obgovorili-osobli vosti-reformi-medzakladiv-vtorinnogo-rivna.html

17. "Автономизация" Академии медицинских наук. URL: http://amnu.gov.ua/avtonomyzac zyya-akademyy-medyczynskyh-nauk

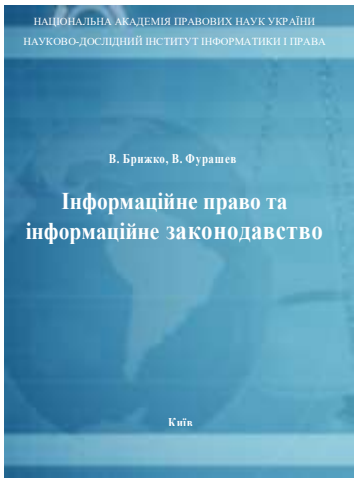
18. О губительных лжереформах Минздрава. – (05.09.2019). URL: https://www.2000.ua/v-nomere/derzhava/realii/avtonomizacija-akademii-medicinskih-nauk.htm

19. Для обговорення стратегія. URL: file:///E:/медицина%20стаття/для%20обговорення %20стратегія.pdf

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

До відома читачів

НОВЕ НАУКОВО-НАВЧАЛЬНЕ ВИДАННЯ



Інформаційне право та інформаційне законодавство: наукове видання / Брижко В.М., Фурашев В.М. – (Рекомендовано до друку Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України, протокол № 7 від 30.10.2019 р.). Київ, 2019. 290 с.

У науковому виданні "Інформаційне право та інформаційне законодавство" на підставі наукових досліджень, проведених авторами впродовж 1998 – 2019 рр. у Національному агентстві з питань інформатизації при Президентові України та НДІПІ НАПрН України (до 2011 р. – НДЦПІ НАПрН України), викладається стан філософських, теоретичних та правових проблем інформаційного права та удосконалення інформаційного законодавства України.

Метою підручника є формування системи сучасних філософсько-гуманітарних, науково-теоретичних та практичних знань щодо методології і методики професійної діяльності ефективного застосування приписів інформаційного права та норм інформаційного законодавства в процесі регулювання суспільних відносин, пов'язаних зі створенням, використанням, обігом та захистом інформації, інформаційних ресурсів, в умовах функціонування інформаційних систем, а також напрямів розробки в державі цілісного інформаційного законодавства.

Для досягнення вказаної мети автори виходять з розмежування категорій "інформаційне право" та "інформаційне законодавство". Перша – закріплює елементи, які визначають принципи та вихідні приписи інформаційно-правових відносин, друга – елементи організаційного поділу законодавчих актів, котрі сформовані в результаті запровадження норм регулювання інформаційних відносин. У загальному плані, "право" інформаційної сфери існує, передусім, для політики, а "законодавство" – для усіх суб'єктів інформаційних відносин.

Зазвичай спілкування супроводжується бажанням інформаційного впливу на свідомість співрозмовника, яка не виключає можливостей маніпулювання думками й фактами. У наш час включення в інформаційно-комунікативні процеси новітніх інформаційних технологій та телекомунікаційних засобів можуть активізувати негативний вплив на психіку окремої людини, а також – на діяльність в інформаційній сфері суспільства й держави, що сприяє руйнуванню генофонду, переформатуванню психології народу, його самоідентифікації й деградації суспільства.

Теоретично-освітнє значення видання "Інформаційне право та інформаційне законодавство" визначається потребами у більш глибокому пізнанні досягнень філософії права, визначенням основних принципів і теоретичних напрацювань, які складають основу формування нової юридичної галузі – "Інформаційне право". Для цього у виданні вперше у освітній діяльності наведено погляди всесвітньо відомих філософів та юристів щодо проблем та перспектив розвитку сфери інформаційного права в контексті "право у філософії пізнання" та "джерела знань філософії права" які визначаються такими поняттями, як "онтологія", "гносеологія", "епістемологія", "логіка", "антропологія",

“аксіологія”, “герменевтика” та “праксеологія”, як основ практичної діяльності у інформаційно-правовій сфері.

Практичне значення видання полягає в визначенні методології комплексного удосконалення інформаційної політики в державі та окреслення пропозицій для рішення основних проблем, пов’язаних з систематизацією і створенням цілісної системи інформаційного права та інформаційного законодавства України.

Видання може бути корисне під час розробки/доповнення навчально-методичних програм та матеріалів з дисциплін, пов`язаних з інформаційним правом та інформаційним законодавством. Також видання може бути корисним всім, хто бажає отримати теоретичні знання і практичні навички у вивченні проблем інформаційного права та удосконаленні нормативно-правового упорядкування суспільних відносин щодо інформації, інформатики, інформатизації в умовах формування інформаційного суспільства.

Якщо Вас, шановні читачі, зацікавило видання, звертайтеся за e-mail адресою:
pravo@ndcpi.org.ua
або
bvm777@ukr.net;
vfurashev@gmail.com

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

РЕЦЕНЗІЯ

на монографію **“Публічне адміністрування національно-безпековою сферою в Україні: теоретико-правові та організаційні засади”** / авт. К.В. Бондаренко

Вітчизняна адміністративно-правова наука потребує розроблення на теоретичному рівні нової категорії, здатної охопити сучасні управлінські процеси та взаємодію правової держави та громадянського суспільства в Україні. Незважаючи на цінність і традиції теорії державного управління та цієї категорії, слід констатувати, державна управлінська діяльність засвідчує застарілість даного поняття. Західна наука пропонує концепції “публічного управління”, “публічного адміністрування”, “демократичного врядування” тощо, які опрацьовуються вітчизняними фахівцями з метою визначення їх змісту, співвідношення, а також можливості їх інтеграції в українське правове поле. Наукові публікації є розрізненими та зазвичай суперечливими, що підкреслює актуальність наукового пошуку у цій сфері. Адміністративно-правова наука потребує вироблення доктринального розуміння категорії, що відповідала б новому державному управлінню у сучасному світі та сучасній Україні зокрема. Тож розроблення автором категорії “публічне адміністрування”, запропоноване автором його розуміння з одного боку є надзвичайно актуальним, з іншого може стати міцним поштовхом для продовження досліджень у цій сфері, виводячи їх на новий рівень.

Особливої уваги потребує, поряд із публічним адмініструванням як процесом, потребує й об’єкт, на який справляється керуючий вплив. Події, що відбуваються у державі та суспільстві, демонструють об’єктивну необхідність аналізу публічного адміністрування саме у сферах, що забезпечують існування та ефективну діяльність держави. Адміністративно-політична сфера, що виокремлювалась у науці адміністративного права, на сьогоднішній день також вичерпала себе, оскільки розмито межі, які б її відокремлювали, та втрачено атрибути сфери. Запропонована автором національно-безпекова сфера є новим поглядом на об’єкт публічного адміністрування, та свідчить про актуальність монографічного дослідження.

Структура роботи є вивіреною та стрункою. Перший розділ присвячено теоретичним засадам публічного адміністрування національно-безпековою сферою, де, серед іншого, здійснено сутнісно-правову характеристику категорії “публічне адміністрування”, а також визначено зміст поняття “національно-безпекова сфера”. Другий розділ логічно продовжує перший та розкриває правові засади публічного адміністрування національно-безпековою сферою, у якому розглянуто як ґенезу законодавства, так і сучасний стан законодавства щодо регулювання відповідною сферою. Структурну-понятійну характеристику національно-безпековою сферою здійснено у третьому розділі, де охарактеризовано об’єкт публічного адміністрування та послідовно розглянуто кожну із галузей сфери – галузі національної безпеки і оборони, закордонних справ, внутрішніх справ, юстиції та публічної служби. Суб’єктам публічного адміністрування присвячено четвертий розділ, у якому розглянуто систему суб’єктів публічного адміністрування національно-безпековою сферою, охарактеризовано особливості статусу суб’єктів публічного адміністрування національно-безпековою сферою вищого рівня, центрального та місцевого рівня. Зміст публічного адміністрування національно-безпековою сферою, а саме форми і методи публічного адміністрування, контрольно-наглядову діяльність, а також сучасний стан здійснення публічного адміністрування розкрито у п’ятому розділі. Тож зміст роботи дозволяє цілісно та послідовно розкрити усі аспекти обраної теми із

визначенням загальнотеоретичних засад, аналізу законодавства, характеристиці елементів публічного адміністрування та його функціонування.

Характеризуючи монографію в цілому, необхідно відмітити її наукову та новизну, цілісність, актуальність; авторський підхід обумовлює цікавий стиль викладення матеріалу. Теоретичний матеріал аргументовано відповідними посиланнями на доктринальні та нормативні джерела, що дає змогу самостійно ознайомитись з окремими питання розглядуваних тем. Також заслуговують на увагу численні посилання на джерела зарубіжних авторів.

Цікавою є пропозиція автора розглядати публічне адміністрування як результат еволюційного розвитку державного управління, що обумовлюється розвитком соціально-організованого суспільства, та яке характеризується зростаючим рівнем демократичності та відкритості, зменшенні безпосереднього розпорядництва та імперативів, зосередженні на сервісній складовій. Такими, що містять наукову новизну, є запропоновані автором визначення базових категорій монографії.

Загалом, коло науково-практичних питань, які розглядаються у монографії, є надзвичайно широким. Безумовно, це свідчить про її високий рівень та науковий інтерес. Разом з тим, велика кількість питань, які зачіпаються у монографічному дослідженні, самі по собі можуть бути розглянуті на дисертаційному рівні. У подальших дослідженнях хотілося б, щоб автор більш детально запинився на характеристиці правового статусу місцевих органів публічної влади як суб'єктів публічного адміністрування, а також аналізи матеріалів їх практичної діяльності.

Отже, монографія К.В. Бондаренко "Публічне адміністрування національно-безпековою сферою в Україні: теоретико-правові та організаційні засади" є комплексною науковою працею, виконаною на актуальну тему, має наукову й практичну цінність. Думається, що результати дослідження можуть бути використані при викладанні курсів "адміністративне право", "публічне адміністрування", а також в теоретичних дослідженнях з проблем національної безпеки та публічного адміністрування.

Професор кафедри адміністративного та інформаційного права
Навчально-наукового інституту права, психології та інноваційної освіти
Національного університету "Львівська політехніка",
доктор юридичних наук, професор Л. Чистоклетов

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ПЕРЕЛІК СТАТЕЙ,

опублікованих у журналі ІНФОРМАЦІЯ І ПРАВО у 2019 р.

№ з/п	Назва статті	Автор(и)	№ журналу, стор.
Інформаційне право			
1	Сучасна людина: безпекові проблеми адаптації до нового інформаційного середовища	Дзьобань О.П. Рубан О.О.	1(28)/2019, с. 9-18
2	Право на відкриті дані – як право приватного характеру	Корж І.Ф.	1(28)/2019, с. 19-28
3	Цифровий розвиток та національна безпека у контексті правових проблем	Доронін І.М.	1(28)/2019, с. 29-36
4	Інформаційний делікт як підстава "інформаційної" юридичної відповідальності: відмітні ознаки	Тихомиров О.О.	1(28)/2019, с. 37-44
5	Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері	Кушнір І.П.	1(28)/2019, с. 45-51
6	Правові особливості інформаційних суспільних відносин при наданні дистанційних адміністративних послуг	Кравчук І.М.	1(28)/2019, с. 52-60
7	Правовий статус роботів: проблеми та перспективи визначення	Бежевець А.М.	1(28)/2019, с. 61-67
8	Національна інтегрована система нормативно-правових актів: реальність і можливості	Корж І.Ф.	2(29)/2019, с. 9-17
9	Сутність і зміст законодавства у секторі оборони та його реалізації: інформаційно-правове дослідження	Довгань О.Д. Ященко В.А.	2(29)/2019, с. 17-25
10	Інформаційні права: теоретичні та системні положення	Селезньова О.М.	3(30)/2019, с. 9-15
11	Інформаційна та національна культури українського соціуму: проблеми кореляції	Дзьобань О.П. Прудникова О.В.	3(30)/2019, с. 16-27
12	Філософія права: праксеологія в сфері інформаційного права	Брижко В.М.	3(30)/2019, с. 28-34
13	Доступ громадян до правової інформації: механізми доступу та їх реалізація	Корж І.Ф.	3(30)/2019, с. 35-43
14	Правовий режим доступу до інформації	Семенюк О.Г. Леонов Б.Д.	3(30)/2019, с. 44-49
15	Комерційна таємниця як вид інформації з обмеженим доступом: аналіз законодавчої практики	Свинарчук В.М.	3(30)/2019, с. 50-54
16	Інформаційні правовідносини в судочинстві України	Фурашев В.М. Солончук І.В.	3(30)/2019, с. 55-64
17	Директива 2019/790/ЄС про авторське право в єдиному цифровому ринку та питання адаптації законодавства України	Капіца Ю.М.	3(30)/2019, с. 65-77
18	Відповідальність: до проблеми концептуалізації категорії	Дзьобань О.П., Рубан О.О.	4(31)/2019, с. 9-19
19	Права і свободи людини і громадянина: концептуальні підходи до диференціації в ФРГ та Україні	Косілова О.І., Федірко І.П.	4(31)/2019, с. 20-27
20	Інформаційні правовідносини: поняття та охорона	Солончук І.В.	4(31)/2019, с. 28-36
21	Цифрова культура та інформаційна культура: права людини в епоху цифрових трансформацій	Головко О.М.	4(31)/2019, с. 37-44

22	Проблеми визначення правового режиму об'єктів, створених за допомогою технологій нейромереж	Дубняк М.В.	4(31)/2019, с. 45-53
Правова інформатика			
23	Резонансні явища в системах Інтернету речей	Брайчевський С.М.	1(28)/2019, с. 68-73
24	Побудова онтологій в галузі права за даними сервісу Google Scholar	Ланде Д.В. Дмитренко О.О. Радзієвська О.Г.	1(28)/2019, с. 74-85
25	Мережева модель правових обмежень доступу до Інтернету у світі	Ланде Д.В. Ліненко Ю.О.	2(29)/2019, с. 26-31
26	Зворотні зв'язки в системах Інтернету речей з елементами штучного інтелекту	Брайчевський С.М.	2(29)/2019, с. 32-39
27	Юридична освіта та сфера надання правових послуг в контексті штучного інтелекту	Радутний О.Е.	2(29)/2019, с. 40-54
28	Електронний парламент як базис побудови національної системи нормативно-правових актів	Дорогих С.О.	2(29)/2019, с. 55-59
29	Мораль і право для штучного інтелекту та цифрової людини: закони робототехніки та "проблема вагонетки"	Радутний О.Е.	3(30)/2019, с. 78-95
30	Особливості суб'єктного складу інформаційних відносин в умовах Індустрії 4.0	Бежевець А.М.	4(31)/2019, с. 54-60
31	Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту	Брайчевський С.М.	4(31)/2019, с. 61-67
32	Особливості правового регулювання електронних господарських договорів в Україні	Маньгора В.В.	4(31)/2019, с. 68-72
Інформаційна і національна безпека			
33	Система інформаційної безпеки України: онтологічні виміри	Довгань О.Д. Ткачук Т.Ю.	1(28)/2019, с. 86-99
34	Актуальні проблеми забезпечення інформаційної безпеки електоральних процесів: аналіз зарубіжного досвіду	Гребенюк М.В. Леонов Б.Д.	1(28)/2019, с. 100-107
35	Аналіз стану кіберзлочинності в Україні	Гавловський В.Д.	1(28)/2019, с. 108-117
36	Сучасні тенденції організованої кіберзлочинності	Гуцалюк М.В.	1(28)/2019, с. 118-128
37	Стан та проблемні питання реалізації Стратегії кібербезпеки України	Ткачук Н.А.	1(28)/2019, с. 129-134
38	Від "інформаційного суспільства до "інформаційної безпеки": до проблеми концептуалізації сутності понять	Дзьобань О.П. Жданенко С.Б.	2(29)/2019, с. 60-73
39	Правові проблеми суверенізації Інтернету	Доронін І.М.	2(29)/2019, с. 74-81
40	Проблеми протидії поширенню деструктивної пропаганди та дезінформації напередодні виборів: аналіз досвіду ЄС	Гребенюк М.В. Леонов Б.Д.	2(29)/2019, с. 82-89
41	Оцінка реалізації стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик	Гуцалюк М.В.	2(29)/2019, с. 90-99
42	Повноваження СБ України як суб'єкта національної системи кібербезпеки	Петров С.Г.	2(29)/2019, с. 100-105
43	Щодо деяких підходів до вдосконалення контррозвідувального пошуку органів військової контррозвідки СБ України з урахуванням аналізу законодавства США	Кравченко Р.М.	2(29)/2019, с. 106-114

44	Сутність та зміст розслідування кіберінцидентів та кібератак підрозділами СБ України	Кулешов М.В.	2(29)/2019, с. 115-122
45	Удосконалення законодавства та навчальної програми викладання предмета *"*Захист Вітчизни*"* в середніх загальноосвітніх закладах	Сандул В.С.	2(29)/2019, с. 123-128
46	Проблеми правового регулювання та розвиток кібернетичної безпеки України на сучасному етапі	Костенко О.В.	3(30)/2019, с. 96-104
47	Захист інформації шляхом посилення ефективності протидії кібератакам	Гавловський В.Д.	3(30)/2019, с. 105-110
48	Досвід НАТО з формування змісту інформаційно-аналітичної компетентності співробітників альянсу в ракурсі стратегічного планування	Волобуєва Г.М.	3(30)/2019, с. 111-118
49	Маніпуляції свідомістю людини як основний спосіб ведення передвиборчих кампаній	Фурашев В.М., Самчинська О.А.	3(30)/2019, с. 119-125
50	Військово-патріотичне виховання при викладанні навчального предмета *"*Захист Вітчизни*"* в середніх загальноосвітніх закладах	Сандул В.С., Сікорський В.А.	3(30)/2019, с. 126-131
51	Співвідношення інформаційної та кібернетичної безпеки	Тарасюк А.В.	4(31)/2019, с. 73-82
52	Правова безпека сфери доступу громадян до управління державними справами	Корж І.Ф.	4(31)/2019, с. 83-92
53	Соціологічні дослідження у виборчому процесі як чинник інформаційної безпеки	Золотар О.О.	4(31)/2019, с. 93-97
54	Удосконалення методичного забезпечення експертних досліджень спеціальних програмних засобів у сфері протидії кіберзлочинності	Леонов Б.Д., Серьогін В.С.	4(31)/2019, с. 98-106
55	Правові основи взаємодії державних органів та приватних суб'єктів із метою захисту електронних інформаційних ресурсів України	Петров С.Г.	4(31)/2019, с. 107-112
56	Можливості адаптації іноземного правового забезпечення діяльності та організаційної побудови органів військової контррозвідки	Кравченко Р.М.	4(31)/2019, с. 113-118
Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – "Право"			
57	Виключні особливості розвитку інституту усиновлення у вітчизняному цивільному процесуальному праві	Тубольцева Я.С.	1(28)/2019, с. 135-143
58	Право на інформацію щодо альтернативних методів вирішення спорів	Головко О.М.	1(28)/2019, с. 144-151
59	Перші кроки відновлення роботи органів юстиції на визволеній від нацистів території України (1943–1944 рр.)	Беланюк М.В. Вронська Т.В.	2(29)/2019, с. 129-140
60	Недоторканність народного депутата України – конституційно-правова гарантія незалежного парламентського контролю: інформаційно-правовий аспект	Нижник А.І.	2(29)/2019, с. 141-155
61	Правова культура молоді в Україні	Уханова Н.С.	2(29)/2019, с. 156-165
62	Міграційний режим перебування іноземних громадян і осіб без громадянства на території України: стан і перспективи	Бєлєвцева В.В.	2(29)/2019, с. 167-171
63	Перспективи створення спеціальних правових режимів для трудових мігрантів	Денисов А.І.	2(29)/2019, с. 172-178

64	Публічний контроль за забезпеченням прав викривачів	Косиця О.	2(29)/2019, с. 179-185
65	Дискусійні питання місця виконавчого провадження в системі права України	Лимарь І.В.	2(29)/2019, с. 186-193
66	Особливості суб'єктного складу у справах про усиновлення	Тубольцева Я.С.	3(30)/2019, с. 132-139
67	Трансформація системи охорони здоров'я в Україні	Беланюк М.В., Радзієвська О.Г., Маньгора Т.В.	4(31)/2019, с. 119-128
Нове науково-навчальне видання: **Інформаційне право та інформаційне законодавство**: наукове видання / Брижко В.М., Фурашев В.М. – (Рекомендовано до друку Вченою радою Науково-дослідного інституту інформатики і права Національної академії правових наук України, протокол № 7 від 30.10.2019 р.). Київ, 2019. 290 с.			4(31)/2019, с. 129-130
Рецензія на монографію: **Публічне адміністрування національно-безпековою сферою в Україні: теоретико-правові та організаційні засади** / автор К.В. Бондаренко; рецензент професор кафедри адміністративного та інформаційного права Навчально-наукового інституту права, психології та інноваційної освіти Національного університету "Львівська політехніка", доктор юридичних наук, професор Л. Чистоклетов			4(31)/2019, с. 131-132

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

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 напрямами 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.

   • 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 ПІБ 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 вичитаними, 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 370 грн. на рахунок Інституту**.

Реквізити для оплати робіт:
Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 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 НДІІП 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 додержання 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

№ 4(31)/2019

Засновники журналу:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІІП НАПрН України); - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини "Україна".
Видавець:	© НДІІП 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 – НДІІП НАПрН України; URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.

Founders of journal:	- 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.