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(27)/2018

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(27)/2018

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

КОРЖ І.Ф. Децентралізація та її вплив на розвиток регіональних суспільних відносин ……..**9**

МАРУЩАК А.І., ПЕТРОВ С.Г. Зміст поняття “державні електронні інформаційні ресурси”…….……**15**

ЯЦИШИН М.Ю. Використання сили у кіберпросторі в рамках міжнароднго права……...**22**

УХАНОВА Н.С. Виклики і загрози правам та безпеці людини в інформаційній сфері……...**33**

Правова інформатика

БАРАНОВ О.А. Інтернет речей (IoT): регулювання надання послуг роботами зі штучним інтелектом…….…….....…**46**

БРАЙЧЕВСЬКИЙ С.М. Узагальнення індексу цитування як компенсація неповноти наукометричних база даних…….……**71**

Інформаційна і національна безпека

ДОВГАНЬ О.Д., ТКАЧУК Т.Ю. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права…….……**79**

ДОРОНІН І.М. Оборонні “Білі книги”: правові аспекти інформування суспільства про діяльність сектору безпеки і оборони у контексті громадського контролю……..…….....**90**

ЄВТУШЕНКО Є.В., ЛЕОНОВ Б.Д. Захист від недобросовісної конкуренції: нормативно-правовий та інформаційний аспекти…….….**98**

ТКАЧУК Н.А. Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки……**104**

КРАВЧЕНКО Р.М. Діяльність військової контррозвідки в Армії США: організаційно-правовий аспект……..**112**

КВАСЮК В.В. Основні підходи до визначення поняття “біотероризм”……...… **121**

ВЕРГОЛЯС О.О. Інформаційне-правове забезпечення спеціальних інформаційних операцій…….. **126**

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

НИЖНИК А.І. Сучасні тенденції надання комітетам Верховної Ради України спеціальних повноважень для здійснення парламентського контролю: організаційно-правовий аспект……..…….**134**

ЖИРОВА П.О. Запобігання торгівлі людьми в Україні:
міжнародні стандарти та стан реалізації……..….**143**

До відома читачів

Перелік статей, опублікованих у журналі ІНФОРМАЦІЯ І ПРАВО у 2018 р….. **150**

До відома авторів ……..…….....**154**

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. 13.6. 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 від 26.12.18 р. № 10

TABLE OF CONTENTS

Informative Law

KORZH I. Decentralization and its influence on the development of regional social relations……..…**9**

MARUSHCHAK A., PETROV S. The meaning of the term "State Electronic Information Recourses"……..……..…**15**

YATSYSHYN M. The use of force in cyberspace under international law…….. **22**

UHANOVA N. Challenges and threats to the human rights and safety in an information sphere……..…**33**

Legal Informatics

BARANOV O. Internet of Things (IoT): regulation of the provision of services by robots with artificial intelligence……....…..... **46**

BRAYCHEVSKYY S. Generalization of the science citation index as a compensation for the incompleteness of scientometric datebases…….**71**

Informative and National Safety

DOVGAN O., TKACHUK T. Scientfic reflexion of the information security of Ukraine: from positivism to metaphysics of the law….. **79**

DORONIN I. White Books in the field of defense: legal aspects of informing society about activity of the security and defense sector in the context of civilian control……..……..….**90**

IVTUHENCO I., LEONOV B. Protection against unfair competition: regulatory and information aspects……..……...**98**

TKACHUK N. Legal regulation of interaction between Security Service of Ukraine and a private sector in the field of providing cyber security…..……. **104**

KRAVCHENKO P. Activity of military counter-intelligence in the USA Army: organizational and legal aspect……..……**112**

KVASIUC V. Basic approaches to the deffiniton of concept "bioterrorism"…….…. **121**

VERHOLIAS O. The information and legal provision of special information operations… **126**

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

NIZHNIK A. The current trends to empower the Committees of the Verkhovna Rada of Ukraine with special authority in the sphere of parliamentary control: organizational and legal aspect…… **134**

ZHYROVA P. Prevention of People Trafficking in Ukraine:
International Standards and Implementation…….... **143**

For the consideration of readers

List of articles published in the journal INFORMATION AND LAW in 2018…….. **150**

For the consideration of authors ……..……..... **154**

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol dated 26.12.18 № 10

Інформаційне право

УДК 353.2(5)

КОРЖ І.Ф., *доктор юридичних наук,* завідувач науковою лабораторією НДІІП НАПрН України

ДЕЦЕНТРАЛІЗАЦІЯ ТА ЇЇ ВПЛИВ НА РОЗВИТОК РЕГІОНАЛЬНИХ СУСПІЛЬНИХ ВІДНОСИН

Анотація. *В даній статті досліджуються питання становлення та напрями подальшого розвитку суспільно-правових відносин в умовах децентралізації державної влади та здійснення реформи місцевого самоврядування в Україні; розкриваються проблемні питання реформ і їхній вплив на муніципально-правові відносини в територіальних громадах України.*

Ключові слова: *державне управління, децентралізація, муніципальне право, муніципально-правові відносини, органи місцевого самоврядування, територіальні громади.*

Summary. *This article explores the formation and directions of further development of socio-legal relations in the conditions of state power decentralization and implementation of the reform of local self-government in Ukraine; reveals the problematic issues of reforms and their influence on the municipal and legal relations in the territorial communities of Ukraine.*

Keywords: *governance, decentralization, municipal law, municipal and legal relations, local governments, territorial communities.*

Аннотация. *В данной статье исследуются вопросы становления и направления дальнейшего развития общественно-правовых отношений в условиях децентрализации государственной власти и осуществления реформы местного самоуправления в Украине; раскрываются проблемные вопросы реформ и их влияние на муниципально-правовые отношения в территориальных общинах Украины.*

Ключевые слова: *государственное управление, децентрализация, муниципальное право, муниципально-правовые отношения, органы местного самоуправления, территориальные общины.*

Постановка проблеми. В Україні розпочато децентралізацію державної влади та започатковано здійснення ряду важливих реформ, однією з яких є реформа місцевого самоврядування. У суспільстві до цього часу ще точаться дискусії щодо їх доцільності та можливої результативності. Однак дедалі відчутнішими й очевидними стають їх результати, дедалі більшу повагу виявляють до органів місцевого самоврядування органи державної влади. Визнання територіальних громад первинними суб'єктами місцевого самоврядування, основним носієм його функцій і повноважень, надання якісно нового статусу місцевим радам тощо – змінило не лише механізм здійснення публічної влади на місцях, а й політичну систему всього українського суспільства.

Становлення місцевого самоврядування супроводжується розвитком законодавства у цій галузі, багатою локальною нормотворчістю і ратифікацією відповідних міжнародно-правових актів. Закономірним наслідком цього нормотворчого процесу є становлення якісно нового інституту конституційного права та нової галузі права – муніципального права України, основними джерелами якого є Конституція України, закони України "Про місцеве самоврядування в Україні" та "Про службу в органах місцевого самоврядування", Європейська Хартія про місцеве самоврядування, Конституція Автономної Республіки Крим, Закон України "Про столицю України – місто-герой Київ".

Реалізація муніципального права, його подальший розвиток і вдосконалення, має бути в центрі уваги науковців, їхніх наукових досліджень. Вивчення і вдосконалення муніципальних правовідносин, виявлення "слабких" їх місць, – належний вклад у справу побудови демократичної, соціальної, правової держави, допомога у залученні українського народу до когорти розвинутих, демократичних і вільних народів світового співтовариства.

Метою статті є дослідження питання становлення та напрацювання шляхів подальшого розвитку муніципальних правовідносин у період реформи місцевого самоврядування в Україні; розкриття відповідних проблем та напрацювання шляхів їх усунення.

Виклад основного матеріалу. Питання децентралізації державного управління в Україні стояло на порядку денному українського життя з моменту вибору нашої незалежності. Та модель, яка дісталася незалежній Україні у спадок потребувала реформи, зміни своєї сутності, оскільки радянській моделі місцевого самоврядування були притаманні наступні риси:

– державність органів місцевого самоврядування, які являли собою "нижній поверх" державного механізму;

– фактична відсутність власної компетенції;

– жорстка централізація управління;

– принцип патерналізму, що виражався у слабкості і нерозвинутості структур громадянського суспільства та присутності "сильної" державної влади, яка узурпуючи багато суспільних функцій, обслуговує суспільство і особистість сукупністю дріб'язкових норм, регламентацій і приписів, тощо.

Таким чином, радянська модель самоврядування фактично не відповідала своєму значенню, не мала в собі відповідних механізмів для підтримання та розвитку своєї життєдіяльності, окрім централізованої підтримки та управління. Суспільні відносини між так званим центром і регіонами будувалися на принципах підпорядкування і звітування, підтримки центру та визначення центром обсягу цієї підтримки. Тому перед молодою країною постало завдання привести дану систему у відповідність до європейських стандартів.

Так, у липні 1997 року Верховною Радою України була ратифікована Європейська хартія місцевого самоврядування від 15 жовтня 1985 року [1], яка була прийнята під егідою Конгресу Місцевих та Регіональних Влад Європи та набрала чинності 1 вересня 1988 року, і тим самим була задекларована відданість європейським стандартам управління. Європейська Хартія місцевого самоврядування є першим багатостороннім правовим документом, який визначає і захищає принципи місцевої автономії – однієї з підвалин демократії.

Прийняттю даної Хартії передувало прийняття Всесвітньої Декларації місцевого самоврядування [2]. Вона була прийнята XXVII Конгресом Міжнародної Спілки місцевої влади 26 вересня 1985 року в Ріо-де-Жанейро і значною мірою збігається з положенням Європейської хартії. Незважаючи на її необов'язковість для виконання Україною, вона становить значний інтерес, оскільки в ній знайшла свій відбиток і закріплення позиція широких кіл світової громадськості, активістів і спеціалістів муніципального руху з питань становлення і функціонування локальної демократії.

З тих пір було зроблено декілька спроб провести необхідні реформи, але в силу різних причин вони не були успішними. Втілення в життя системних змін почалося відразу після подій на Майдані, а саме: 1 квітня 2014 року Кабінетом Міністрів України було прийнято Концепцію реформування місцевого самоврядування та територіальної

організації влади [3]. Після цього був затверджений План заходів щодо її реалізації, які дали старт реформі [4] і який діяв до 2016 року і був замінений на новий План [5].

Децентралізація сама по собі – це процес передачі повноважень і бюджетних надходжень від органів державної влади до органів місцевого самоврядування. Українська децентралізація має три складові:

– реформа територіальної організації влади;

– реформа місцевого самоврядування;

– реформа регіональної політики.

Зазначені складові децентралізації мають докорінно змінити суспільні відносини як в самих регіонах, так і у відношеннях між центром і регіонами. Якщо раніше ці відносини мали явну ознаку імперативності, повсюдності рішень центру, за яких центр диктував умови функціонування регіонів, їх фінансував, то після завершення децентралізації вони мають набути ознаки своєрідного партнерства, тобто фокус прийнятих рішень щодо регіонів зміститься у бік самих регіонів.

Таким чином, основним завданням децентралізації є створення умов для розвитку громад та наближення послуг до людей шляхом формування заможних громад, передачі більшої частини повноважень на базовий рівень управління та чіткого розмежування функцій між рівнями управління, а також гарантування належного ресурсного забезпечення місцевого самоврядування.

Першим кроком до зміни суспільних відносин у сфері місцевого самоврядування має бути зміна правил їх регулювання, тобто, реформування так званого муніципального законодавства, або право місцевого самоврядування, що включає в себе: Конституцію України; закони України "Про місцеве самоврядування", "Про столицю України – місто-герой Київ"; міжнародно-правові акти в галузі місцевого самоврядування, що зазначені вище; нормативно-правові акти суб'єктів системи місцевого самоврядування (акти місцевих референдумів, статути, регламенти відповідних рад); нормативно-правові договори за участю суб'єктів системи місцевого самоврядування. Крім того, необхідно було напрацювання ряду законів та підзаконних актів для врегулювання муніципальних відносин у процесі здійснення децентралізації.

Муніципально-правові норми є первинними елементами системи муніципального права. Їх класифікують залежно від різних якостей, наприклад за юридичною силою (конституційні, законодавчі, підзаконні, норми міжнародно-правових актів). На підставі муніципально-правових норм виникають ***муніципально-правові відносини,*** під якими розуміють відносини між двома і більше суб'єктами, які наділяються взаємними правами й обов'язками щодо здійснення муніципальної влади. Важливо також підкреслити, що муніципальне право розглядається не тільки як галузь права та законодавства, а й як юридична наука та навчальна дисципліна. Таким чином ***муніципальне право*** – це система норм, які регулюють суспільні відносини у сфері місцевого самоврядування та інші тісно пов'язані з ними суспільні відносини. Тому можна стверджувати, що муніципальне право стосується, насамперед, безпосередньої і представницької місцевої (локальної) влади, а отже, воно належить до групи публічних галузей права [6, с. 281].

Предметом муніципального права є суспільні відносини, пов'язані з організацією і функціонуванням місцевого самоврядування як самостійного та відносно відокремленого виду публічної локальної влади в системі народовладдя в межах певних адміністративно-територіальних одиниць.

Муніципальне право належить до групи публічних галузей права. Його норми регулюють і охороняють, насамперед, відносини влади, пріоритетними серед яких є

зобов'язання. Отже, ***методом муніципального права*** є загальне зобов'язання, для якого характерна імперативність, тобто підпорядкованість однієї зі сторін правових відносин. Разом із тим, диспозитивний метод, під яким розуміють юридичну рівність сторін, може застосовуватися у відносинах суміжних або дуже близьких до чисто муніципальних, наприклад у договірних відносинах органів і посадових осіб місцевого самоврядування з іншими юридичними і фізичними особами.

Надзвичайно важливим методом у системі муніципального права є метод децентралізації (передачі) владних повноважень від держави до територіальної громади як інституту громадянського суспільства. Безперечно, він використовується спільно з методами централізації, координації і субординації тощо [6, с. 282].

Зазначимо, що суспільні відносини, які регулюються правовими нормами муніципального права, або, іншими словами, муніципально-правові відносини, мають у переважній більшості спільні риси з іншими правовідносинами і, насамперед, з конституційно-правовими, адміністративно-правовими, фінансово-правовими, оскільки муніципальне право є комплексною галуззю публічного права й інститутом конституційного права.

Муніципально-правові відносини за своїм змістом і формами, умовами функціонування і розвитку та іншими знаками є багатогранними.

Разом з тим, муніципально-правові відносини мають ряд особливостей, зокрема щодо територіальної сфери цих відносин, щодо суб'єктів і об'єктів, значне коло яких не характерне для інших правовідносин, а також щодо прав і обов'язків суб'єктів цих відносин та їх форм. Пріоритетним видом муніципально-правових відносин є відносини безпосереднього народовладдя, основними формами яких вважаються місцеві референдуми, місцеві вибори, місцеві ініціативи тощо.

Головну частину муніципально-правових відносин складає, звичайно, діяльність представницьких органів місцевого самоврядування – сільських, селищних, міських, районних і обласних рад, виконавчих органів сільських, селищних, міських рад і сільських, селищних і міських голів.

Муніципально-правові відносини можуть поділятися також за своїм змістом на матеріальні і процесуальні, за формою – на організаційні і правові; за часом – на короткострокові й довгострокові; за простором – на місцеві та регіональні; за правовою природою – на правомірні та протиправні.

Підставами виникнення, зміни та припинення муніципально-правових відносин, як і інших правовідносин, є юридичні факти, що поділяються на дії та події.

Оскільки муніципально-правові відносини – це насамперед і головним чином публічні, владні відносини, які ґрунтуються на природному праві жителів сіл, селищ, міст самостійно вирішувати питання місцевого значення, основними юридичними фактами, що зумовлюють їх (муніципально-правових відносин) виникнення, зміну та припинення, є дії, зокрема прийняття актів суб'єктами системи місцевого самоврядування [7, с. 26].

Основними суб'єктами муніципально-правових відносин є: Український народ, Українська держава; органи державної влади; політичні партії і громадські організації, їх об'єднання і осередки; громадяни України; територіальні громади, жителі відповідних адміністративно-територіальних одиниць; представницькі органи місцевого самоврядування (місцеві ради), виконавчі органи місцевих рад; сільські, селищні, міські голови, органи самоорганізації населення, депутати місцевих рад, посадові особи місцевого самоврядування, підприємства, установи, організації; асоціації та інші об'єднання органів місцевого самоврядування; юридичні особи.

Основними об'єктами муніципально-правових відносин є: влада народу; права, свободи і інтереси людини і громадянина; влада територіальних громад; питання місцевого значення; функції (напрями і види діяльності) суб'єктів місцевого самоврядування; об'єкти комунальної власності; місцеві бюджети, доходи місцевих бюджетів, місцеві податки і збори, місцеві позики; природні блага, природні об'єкти, природні ресурси, об'єкти природно-заповідного фонду, земля; духовні блага (освіта, наука, культура, інформація, пам'ятки історії, культури, архітектури, містобудування); соціальні блага (об'єкти житлово-комунального господарства, побутового, торговельного обслуговування, громадського харчування, транспорту і зв'язку, охорони здоров'я, фізкультури і спорту тощо); програми економічного та соціально-культурного розвитку сіл, селищ, міст і цільові програми з інших питань самоврядування; плани підприємств і організацій; адміністративно-територіальний устрій тощо.

Складовою частиною об'єктів муніципально-правових відносин є статус, компетенція, повноваження, суб'єктивні права та юридичні обов'язки суб'єктів муніципально-правових відносин, їх гарантії і відповідальність. Зокрема, Конституцією і Законом України "Про місцеве самоврядування в Україні" визначається статус територіальних громад, місцевих рад як представницьких органів місцевого самоврядування, виконавчих органів рад, сільського, селищного чи міського голови, органів самоорганізації населення.

У процесі децентралізації муніципально-правові відносини змінюються, набувають нового формату. Відповідно до Концепції [3] та до інших актів, які регулюють питання децентралізації в Україні, згадані відносини змінюються під впливом наступних факторів: створення нових територіальних та об'єднаних територіальних громад (станом на початок вересня 2018 року створено вже 838 об'єднаних територіальних громад (далі – ОТГ), з яких 133 ОТГ чекають на призначення перших виборів. До складу цих ОТГ увійшли **3839** колишніх **місцевих рад**; більше **7,1** млн. людей проживають в ОТГ) [8]; запровадження посади старости (в селах ОТГ працюють вже 780 старост, ще майже 1,8 тисяч осіб виконують обов'язки старост); розширення співробітництва, включаючи міжнародне, територіальних громад (реалізується вже **263 договори** про співробітництво. Цим механізмом скористалися **1050 громад**); розширення діапазону суб'єктів, які наповнюють місцеві бюджети (місцеві бюджети за останні роки зросли на **123,4 млрд грн**: з 68,6 млрд в 2014 до 192 млрд грн в 2017 році); отримання повноважень у сфері архітектурно-будівельного контролю (нові містобудівні повноваження отримали 100 міст, в тому числі – 12 ОТГ); отримання повноваження з надання базових адміністративних послуг (реєстрацію місця проживання, видачу паспортних документів, державну реєстрацію юридичних та фізичних осіб, підприємців, об'єднань громадян, реєстрацію актів цивільного стану, речових прав, вирішення земельних питань тощо).

Нова законодавча база значно посилила тенденцію до муніципальної консолідації, започаткування нових і зміни попередніх муніципальних відносин, що направлені на вирішення нагальних проблем. Також фінансові відносини отримали поштовх до існування певних автономних відносин, залежність від центрального бюджету.

Очікується, що 2018 рік стане ключовим у питанні формування базового рівня місцевого самоврядування, тих відносин, що існували до того часу: до кінця року можуть з'явитися нові відносини у зв'язку із об'єднанням більшості існуючих малочисельних місцевих рад та отриманням, у зв'язку з цим, нових повноважень, що дозволить належним чином використовувати ресурси і нести відповідальність за свої дії чи бездіяльність як перед громадянами, так і перед державою. Зазначене створить

підґрунтя для наступних змін у реформі та започаткування нових правовідносин у сфері охорони здоров'я, освіти, соціальних послуг, енергоефективності та в інших сферах.

Зазначені, нові і ті муніципальні правовідносини, що будуть виникати, мають бути врегульовані новими нормативно-правовими актами, положення яких будуть враховувати нові зміни у житті місцевого самоврядування. Так потребує нового врегулювання питання: проходження служби в органах місцевого самоврядування; щодо проведення місцевого референдуму; врегулювання відносин, пов'язаних з уточненням адміністративно-територіального устрою України; щодо відносин, пов'язаних з управлінням земельними ресурсами в межах території об'єднаних територіальних громад; пов'язаних з регулюванням містобудівної діяльності; державного нагляду за законністю рішень органів місцевого самоврядування; щодо відносин, якими будуть регулюватися питання визначення організаційно-правових засад формування міських агломерацій територіальними громадами сіл, селищ і міст, у тому числі об'єднаними територіальними громадами, принципи і механізми взаємодії територіальних громад в межах міських агломерацій, а також форм підтримки державою міських агломерацій тощо.

Висновки.

Підсумовуючи викладене, зазначимо, що в нинішніх умовах муніципальні відносини в Україні отримують новий поштовх до свого розвитку. Адаптація законодавства України до європейського, здійснювані в Україні реформи сприяють розвитку згаданих відносин, насамперед, в інтересах населення територіальних та об'єднаних територіальних громад. Ці відносини набувають нових кольорів і значень, нового змісту, розширення кола суб'єктів та об'єктів, стають більш імперативними. Їх кількість збільшується і їхнє значення для місцевого населення підвищується. За успішного завершення децентралізації та реалізації реформ в країні, муніципальні відносини стануть визначальними в житті мешканців на території тієї, чи іншої громади.

Використана література

1. Про ратифікацію Європейської хартії місцевого самоврядування: Закон України від 15.07.97 р. *Відомості Верховної Ради України*. 1997. № 38. Ст. 249.

2. Всесвітня декларація місцевого самоврядування. URL: https://pidruchniki.com/15931106/pravo/vsesvitnya_deklaratsiya_mistsevogo_samovryaduvannya (дата звернення: 15.10.2018).

3. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України від 01.04.14 р. № 333-р. *Урядовий кур'єр*. 11.04.14 р. № 67.

4. Про затвердження плану заходів щодо реалізації Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України від 18.06.14 р. № 591-р. *Урядовий кур'єр*. 23.07.14 р. № 131.

5. Деякі питання реалізації Концепції реформування місцевого самоврядування та територіальної організації влади в Україні: Розпорядження Кабінету Міністрів України від 22.11.16 р. № 688-р. *Урядовий кур'єр*. 4.10.16 р. № 186.

6. Правознавство: підручник / за ред. В.В. Копейчикова, А.М. Колодія. Київ: Юрінком Інтер, 2006. 749 с.

7. Муніципальне право України: підручник / В.Ф. Погорілко, О.Ф. Фрицький, М.О. Баймуратов та ін. / за ред. В.Ф. Погорілка, О.Ф. Фрицького. Київ: Юрінком Інтер, 2001. 352 с.

8. Державна політика, законодавчі напрацювання, проміжні результати першого етапу децентралізації влади в Україні. ресурс. URL: https://decentralization.gov.ua/about (дата звернення: 02.11.2018).

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

УДК 341.217:342.52

МАРУЩАК А.І., *доктор юридичних наук, професор*,
директор Навчально-наукового інституту перепідготовки та підвищення кваліфікації кадрів СБУ Національної академії Служби безпеки України
ПЕТРОВ С.Г., *кандидат юридичних наук,* співробітник СБ України

ЗМІСТ ПОНЯТТЯ "ДЕРЖАВНІ ЕЛЕКТРОННІ ІНФОРМАЦІЙНІ РЕСУРСИ"

Анотація. *У статті досліджується зміст поняття "державні електронні інформаційні ресурси". На основі аналізу нормативно-правових актів і поглядів науковців сформульовано відповідне визначення.*

Ключові слова*: інформація, ресурс, державні інформаційні ресурси, державні електронні інформаційні ресурси.*

Аннотация. *В статье исследуется содержание понятия "государственные электронные информационные ресурсы". На основании анализа нормативно-правовых актов и взглядов ученых сформулировано соответствующее определение.*

Ключевые слова: *информация, ресурс, государственные информационные ресурсы, государственные электронные информационные ресурсы.*

Summary. *The article deals with meaning of the term "State Electronic Information Recourses". Appropriate definition is formulated based upon the legal acts and scientific views analysis.*

Keywords: *information, resources, state information recourses, state electronic information recourses.*

Постановка проблеми. У чинних нормативно-правових актах України використовується низка термінів у сфері інформаційно-правових відносин, які не завжди є взаємоузгодженими між собою. Наприклад, "інформаційний ресурс", "державні ресурси", "державні інформаційні ресурси", "державні електронні інформаційні ресурси" тощо. Від змісту відповідних понять залежить обсяг повноважень окремих органів державної влади, відповідальних за формування і здійснення державної інформаційної політики, захист інформації, протидію кіберзлочинності тощо. Таким чином, виникає потреба у науково-теоретичному обґрунтуванні змісту відповідних понять, зокрема поняття "державні електронні інформаційні ресурси".

Результати аналізу наукових публікацій свідчать про те, що питання визначення змісту поняття "державні електронні інформаційні ресурси" було предметом досліджень лише частково. У вітчизняній юридичній літературі науковим розвідкам цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Брижко, В. Бутузов, О. Довгань, В. Пилипчук, О. Юрченко, К. Тітуніна та інші. Крім того, до розкриття даного питання долучалися дослідники технічних наук О. Юдін і С. Бучик. Питання кримінальної відповідальності за несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури розглядав М.В. Плугатир [1]. Серед зарубіжних авторів виокремлюємо роботи таких вчених, як П. Флетчер, З. Недовіч-Будіч, М. Фіні, А. Раябіфард, Я. Вільямсон та інших.

Метою статті є визначення поняття "державні електронні інформаційні ресурси" та його співвідношення з іншими поняттями інформаційного права України, зокрема з поняттям "електронний документ".

Виклад основного матеріалу. У цій роботі поняття "ресурси" використовуємо у класичному значенні, а саме: "ресурси (від франц. ressource – "допоміжні засоби") – запаси, джерела чого-небудь, які можна використати в разі потреби; засіб, можливість, якими можна скористатися в разі необхідності" [2].

Розглянемо підходи законодавця і наукові погляди на питання щодо змісту загального поняття "інформаційні ресурси". Закон України "Про Національну програму інформатизації" визначає інформаційний ресурс як сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо) [3]. Таким чином, формально законодавець не вказує на електронну форму таких документів. Однак, зважаючи на предмет регулювання зазначеного закону, а саме його спрямування на створення умов для задоволення інформаційних потреб громадян та суспільства на основі створення, розвитку і використання інформаційних систем, мереж, ресурсів та інформаційних технологій, які побудовані на основі застосування сучасної обчислювальної та комунікаційної техніки, робимо висновок, що йдеться про електронні інформаційні ресурси.

Стратегія розвитку інформаційного суспільства в Україні у 2013 році визначає інформаційний ресурс як систематизовану інформацію або знання, що мають цінність у певній предметній області і можуть бути використані людиною в своїй діяльності для досягнення певної мети [4]. Це визначення у порівнянні із попереднім відображає усю сукупність інформації (як в електронній формі, так і у паперовій), що потрапляє до обсягу поняття "інформаційні ресурси". Однак, це вступає у протиріччя з обґрунтованими, на нашу думку, ознаками інформаційних ресурсів, які запропоновані І.В. Мукомелою, зокрема:

1) систематизованість за певним критерієм у вигляді документа або масиву документів;

2) матеріальний характер, тобто існування можливе тільки в зафіксованому на матеріальних носіях вигляді (зручному для формування, зберігання, використання, поширення і сприйняття інформації органами чуття людини);

3) їх цінність – відображення значущої інформації для суспільства, держави, особистості;

4) невичерпність, тобто при використанні, поширенні, зберіганні інформаційні ресурси умовно не знищуються;

5) об'єктивна необхідність в досягненні певного результату/цілей [5, с. 194].

Як бачимо, дослідник виділяє однією із ознак інформаційних ресурсів їх матеріальний характер, тобто існування тільки в зафіксованому на матеріальних носіях вигляді. Під подібну характеристику не завжди підпадають знання, які, наприклад, існують у пам'яті людини.

Еволюція змісту поняття "державні інформаційні ресурси" має цікаві особливості нормативного закріплення відповідної дефініції. Так, наприклад, у березні 2014 року у законодавство України внесено наступне визначення: "державні інформаційні ресурси – інформація, яка перебуває у володінні державних органів, військових формувань, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень" [6]. Як бачимо, акцент зроблено на володінні інформацією державними органами і на обробку за їх дорученням фізичними або юридичними особами. З незрозумілих причин до визначення поняття не включено право державних органів на використання і розпорядження такою інформацією. Також не вказано характеристику систематизованості таких відомостей і їх зв'язок з інформаційними технологіями.

Вже у квітні 2014 року зазначені недоліки були виправлені при схваленні нової редакції Закону України "Про Державну службу спеціального зв'язку та захисту інформації України". Закріплено наступне визначення поняття: "державні інформаційні ресурси – систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень" [7].

Зазначимо, що у 2009 році "інформаційні ресурси держави" у науковому обігу визначали як "взаємопов'язану, упорядковану, систематизовану, закріплену на матеріальних носіях інформацію, створену, зібрану на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету" [8]

Законодавство України містить суміжний до досліджуваного термін "національні електронні інформаційні ресурси". Зміст відповідного поняття полягає в наступному: національні (електронні інформаційні – *від Авт.*) ресурси – ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [9]. Як бачимо, державні електронні інформаційні ресурси є одним із видів національних електронних інформаційних ресурсів.

Дослідники питань електронного урядування виділяють чотири основні групи принципів організації національних електронних інформаційних ресурсів: принципи організації державних е-ІР (для державної служби), принципи організації громадянських е-ІР (для громадян), принципи організації підприємницьких (бізнесу) е-ІР (для юридичних осіб), принципи організації е-ІР для міжнародної спільноти (Інтернет-ресурси) [10, с. 130]. Вважаємо, що для державних електронних інформаційних ресурсів важливими є перші три принципи організації у випадках, коли такі ресурси створені (зібрані) за рахунок державного бюджету і використовуються для потреб державного управління, суспільства і окремих юридичних та фізичних осіб.

Дослідники технічної науки вказують на такі характеристики національних інформаційних ресурсів (national information resources) як: 1) віднесення їх до результатів інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави; 2) їх споживчу цінність (політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо) [11].

Перейдемо безпосередньо до розгляду змісту поняття "державні електронні інформаційні ресурси".

У 2011 році у Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, було внесено зміни, згідно з якими "державні електронні інформаційні ресурси" визначалися як "відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством" [12]. Таким чином, вказується на наступні ознаки таких ресурсів: відображення (задокументованість) в електронному вигляді і передбачена законодавством України необхідність захисту.

Концепція формування системи національних електронних інформаційних ресурсів містить визначення "державних ресурсів" (як складової національних електронних інформаційних ресурсів): "ресурси, які є об'єктом права державної власності" [9].

Суттєву видову характеристику державних ресурсів у системі національних електронних інформаційних ресурсів зустрічаємо у Положенні про Національний реєстр електронних інформаційних ресурсів, аналізуючи яке виокремлюємо такі види державних електронних інформаційних ресурсів: кадастри, державні та інші обов'язкові класифікатори, а також інформаційні системи, які забезпечують їх функціонування та використовують інформацію з них (далі – е-ресурси) [13]. Крім того, до Національного реєстру електронних інформаційних ресурсів включаються е-ресурси суб'єктів владних повноважень, а включення до Національного реєстру е-ресурсів приватної форми власності здійснюється на добровільних засадах [14].

Реалізація державної політики у сфері державних ресурсів полягає, зокрема у розв'язанні таких завдань:

– систематизація, забезпечення доступу до наявних державних ресурсів та їх актуалізація;

– формування та забезпечення ефективного використання державних ресурсів органами державної влади;

– вдосконалення нормативно-правової бази, зокрема визначення порядку і умов користування, оплати робіт, пов'язаних з формуванням, використанням, та захистом державних ресурсів;

– координація діяльності органів державної влади і недержавних структур у сфері формування, використання та захисту державних ресурсів.

Причому концептуальний документ вказує на необхідність "сприяти залученню недержавних структур для надання інформаційних послуг з використанням державних ресурсів" [9].

На сьогодні законодавство України містить перелік пріоритетних державних електронних інформаційних ресурсів (хоча і з метою запровадження електронної взаємодії – *від Авт.*). До таких віднесено: Державний земельний кадастр, Державний реєстр актів цивільного стану громадян, Державний реєстр виборців, Державний реєстр загальнообов'язкового державного соціального страхування, Державний реєстр обтяжень рухомого майна, Державний реєстр речових прав на нерухоме майно, Державний реєстр фізичних осіб-платників податків, Електронна система охорони здоров'я, Єдина державна електронна база з питань освіти, Єдина інформаційна система Міністерства внутрішніх справ, Єдиний державний автоматизований реєстр осіб, які мають право на пільги, Єдиний державний демографічний реєстр, Єдиний державний реєстр Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників, Єдиний державний реєстр судових рішень, Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Єдиний реєстр довіреностей, Єдиний реєстр документів, що дають право на виконання підготовчих та будівельних робіт і засвідчують прийняття в експлуатацію закінчених будівництвом об'єктів, відомостей про повернення на доопрацювання, відмову у видачі, скасування та анулювання зазначених документів, Єдиний реєстр об'єктів державної власності, Реєстр платників податку на додану вартість [14].

Саме зазначені реєстри становлять основу державних електронних інформаційних ресурсів з відкритим доступом, такі ресурси є предметом державного захисту. Звичайно, їх перелік з часом буде розширюватися. Такий висновок робимо на основі аналізу деяких концептуальних документів.

Так, наприклад, Концепція розвитку електронного урядування в Україні передбачає розвиток електронної взаємодії суб'єктів владних повноважень на базі системи електронної взаємодії державних електронних інформаційних ресурсів, у тому

числі підключення базових державних реєстрів і баз даних, центрів надання адміністративних послуг, а також розвиток транскордонної електронної взаємодії. Базова інформаційно-телекомунікаційна інфраструктура електронного урядування буде формуватися шляхом запровадження, розвитку та взаємодії таких державних інформаційних та інформаційно-телекомунікаційних систем:

– система електронної взаємодії органів виконавчої влади;

– система електронної взаємодії державних електронних інформаційних ресурсів;

– інтегрована система електронної ідентифікації та аутентифікації;

– електронний кабінет громадянина;

– веб-портал електронного урядування gov.ua, у тому числі єдиний державний веб-портал відкритих даних та єдиний державний портал адміністративних послуг;

– спеціальні захищені мережі передачі даних, у тому числі національної системи конфіденційного зв'язку;

– захищена електронна пошта;

– захищені центри обробки даних, у тому числі з використанням хмарних технологій;

– формування базових державних реєстрів, у тому числі оцифрування паперових носіїв, та покращення якості даних в державних реєстрах.

Крім того, з одним із завдань Концепції розвитку електронного урядування в Україні є визначення єдиних правил та вимог до створення, ведення і функціонування державних електронних інформаційних ресурсів та запровадження національного реєстру електронних інформаційних ресурсів, а також забезпечення захисту інформації в державних електронних інформаційних ресурсах [15].

Концепція розвитку системи електронних послуг в Україні передбачає зокрема запровадження міжвідомчої електронної взаємодії, відкриття доступу до державних інформаційних ресурсів [16]. Таким чином, з часом розширюватиметься обсяг державних електронних інформаційних ресурсів, можливості доступу до них, і, як наслідок, підвищуватимуться вимоги щодо їх захисту від кіберзагроз.

На нашу думку, до обсягу поняття "державні електронні інформаційні ресурси" мають включатися й інші ресурси, що не потрапляють до зазначених вище реєстрів, наприклад, електронна інформаційна система "Електронний Уряд" [17]. У сучасних умовах масованих кібератак проти державних електронних інформаційних ресурсів модифікація інформації (поширення "рейкових" даних) або блокування роботи системи "Електронний Уряд" може завдавати серйозних репутаційних та фінансових збитків як державі, так і громадянам та юридичним особам, оскільки останнім надаються інформаційні та інші послуги шляхом використання цієї системи [18].

Крім того, до обсягу поняття "державні електронні інформаційні ресурси" відносимо також систему електронної взаємодії таких ресурсів, яка забезпечує виконання Закон України "Про адміністративні послуги" [19], і загалом Єдиного державного порталу адміністративних послуг [20].

Оскільки державні електронні інформаційні ресурси створюються відповідно до закону та за рахунок державного бюджету, їх формування, використання та захист є предметом правового регулювання. Дослідники науки державного управління за результатами аналізу державного регулювання у сфері інформатизації іноземних держав визначають, що поряд з державними електронними інформаційними ресурсами врегульовуються також відносини щодо інформаційних та інформаційно-комунікаційних систем органів державної влади, органів місцевого самоврядування,

закладів, підприємств, установ, організацій, що перебувають у державній чи комунальній власності; електронних адміністративних послуг тощо [21]. Безумовно, характерною ознакою державних ресурсів є урегульованість таких відносин на рівні нормативно-правових актів.

Інші дослідники модифікують визначення, пропонують вважати "інформаційні державно-управлінські ресурси" результатом "інтелектуальної діяльності людини, котрі можна безпосередньо реалізувати в суб'єкт-об'єктній взаємодії процесів державного управління" [22].

Дослідники технічних наук пропонують розуміти під "державними електронними інформаційними ресурсами" (state electronic information resources) – державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави" [11]. Визначальними, на думку вчених, є такі ознаки як існування та використання в електронному вигляді, а також спрямованість на задоволення потреб громадян, суспільства, держави.

Висновки.

Підсумовуючи викладене, та з урахуванням визначення поняття "інформація" [23], формулюємо наступне визначення поняття "державні електронні інформаційні ресурси": *систематизована, закріплена на матеріальних носіях і/або відображена в електронному вигляді інформація, право на володіння, використання або розпорядження якою належить державі або яка обробляється фізичними чи юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень, призначена для задоволення потреб громадянина, суспільства, держави*.

Перспективами подальших наукових пошуків визначаємо питання охорони і захисту державних електронних інформаційних ресурсів від протиправних посягань.

Використана література

1. Плугатир М.В. Кримінальна відповідальність за несанкціоноване втручання в роботу державних електронних інформаційних ресурсів та систем, критичних об'єктів національної інформаційної інфраструктури. *Митна справа*. 2014. № 1(91). Ч. 2. Кн. 1. С. 130-136.

2. Великий тлумачний словник сучасної української мови. URL: http://www.lingvo.ua/uk/Internet/uk-ru/ресурси

3. Про Національну програму інформатизації: Закон України від 04.02.98 р. *Відомості Верховної Ради України.* 1998. № 27. Ст. 181.

4. Про схвалення Стратегії розвитку інформаційного суспільства в Україні: Розпорядження Кабінет Міністрів України від 15.05.13 р. № 386-р. *Урядовий кур'єр.* 13.06.13 р., № 105.

5. Мукомела І.В. Інформаційні ресурси та їх вплив на державно-правовий розвиток. *Державне будівництво та місцеве самоврядування*. 2013. Вип. 26. С. 190-202.

6. Про внесення змін до деяких законодавчих актів України у зв'язку з прийняттям Закону України "Про інформацію" та Закону України "Про доступ до публічної інформації": Закон України від 27.03.14 р. № 1170-VII. *Відомості Верховної Ради України*. 2014. № 22. Ст. 816.

7. Про внесення змін до Закону України "Про Державну службу спеціального зв'язку та захисту інформації України": Закон України від 09.04.14 р. № 1194-VII. *Відомості Верховної Ради України*. 2014. № 25. Ст. 890.

8. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту. *Правова інформатика*. № 1(21)/2009. С. 64-70.

9. Про затвердження Концепції формування системи національних електронних інформаційних ресурсів: Розпорядження Кабінету Міністрів України від 05.05.03 р. № 259-р. *Офіційний вісник України*. 2003. № 18. Ст. 864.

10. Приймак Ю. Розвиток електронного урядування в Україні: організація національних електронних інформаційних ресурсів. URL: http://visnyk.academy.gov.ua/wp-content-/upload/2013/11/2011-4-18.pdf

11. Юдін О.К., Бучик С.С. Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія. Київ: НАУ, 2015. 214 с.

12. Про внесення змін до деяких постанов Кабінету Міністрів України з питань доступу до інформації: Постанова Кабінету Міністрів України від 07.09.11 р. № 938. *Урядовий кур'єр*. 13.09.11 р. № 167.

13. Про затвердження Положення про Національний реєстр електронних інформаційних ресурсів: Постанова Кабінету Міністрів України від 17.03.04 р. № 326. *Офіційний вісник України*. 2004. № 11. Ст. 665.

14. Деякі питання організації електронної взаємодії державних електронних інформаційних ресурсів: Постанова Міністрів України від 10.05.18 р. № 357. *Урядовий кур'єр*. 30.05.18 р. № 100.

15. Про схвалення Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 20.09.17 р. № 649-р. *Урядовий кур'єр*. 27.09.17 р. № 181.

16. Про схвалення Концепції розвитку системи електронних послуг в Україні: Розпорядження Кабінету Міністрів України від 16.11.16 р. № 918-р. *Урядовий кур'єр*. 20.12.16 р. № 240.

17. Про заходи щодо створення електронної інформаційної системи "Електронний Уряд": Постанова Кабінету Міністрів України від 24.02.03 р. № 208. *Офіційний вісник України*. 2003. № 9. Ст. 378. Стор. 112.

18. Про затвердження Переліку і Порядку надання інформаційних та інших послуг з використанням електронної інформаційної системи "Електронний Уряд": Наказ Держкомзв'язку та інформатизації від 15.08.03 р. № 149. *Офіційний вісник України*. 2003. № 48. Ст. 2547.

19. Про адміністративні послуги: Закон України від 06.09.12 р. *Відомості Верховної Ради України*. 2013. № 32. Ст. 409.

20. Про затвердження Порядку ведення Єдиного державного порталу адміністративних послуг: Постанова Кабінет Міністрів України від 03.01.13 р. № 13. *Урядовий кур'єр*. 17.01.13 р. № 10.

21. Котелевець Д.М. Модель взаємодії органів державної влади під час регулювання сфери зв'язку та інформатизації. *Теорія та практика державного управління*. 2015. Вип. 1(48). С. 38-44.

22. Пахомова І.А. До питання систематизації інформаційного законодавства на державній службі. *Вісник Харківського національного університету імені В.Н. Каразіна*. Сер. "Право". 2016. Вип. 22. С. 108-112.

23. Про внесення змін до Закону України "Про інформацію": Закон України від 13.01.11 р. *Відомості Верховної Ради України*. 2011. № 32. Ст. 313.

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

УДК 341.48/.49

ЯЦИШИН М.Ю., старший викладач кафедри міжнародного права
Навчально-наукового інституту міжнародних відносин
Національного авіаційного університету

ВИКОРИСТАННЯ СИЛИ У КІБЕРПРОСТОРІ В РАМКАХ МІЖНАРОДНОГО ПРАВА

Анотація. *У статті досліджується питання міжнародно-правової кваліфікації кібервоєн. Розглядається співвідношення понять "кібератака", "кібернапад", "кіберзлочин" та "кібервійна", на підставі чого автор пропонує власні дефініції. Детально аналізуються підстави застосування норм міжнародного гуманітарного права і міжнародного кримінального права до кібервоєн. Досліджується проблеми поширення дії основних принципів міжнародного права у кіберпросторі. Автор акцентує увагу на кваліфікаційних ознаках, відповідно до яких акти кібервійни можуть бути визнані злочином агресії.*

Ключові слова: *кібервійна, кіберзлочинність, інформаційно-комунікаційні технології, злочин агресії, основні принципи міжнародного права.*

Summary: *The article deals with the issues of international legal qualification of cyberwar. The correlation between the concepts of "cyberattack", "cybercrime" and "cyberwar (cyberwarfare)" is considered. On this basis, the author offers his own distinctions. The reasons for applying international humanitarian law and international criminal law norms to cyberwar are analyzed in detail. The article deals with the problem of extending the basic principles of international law in cyberspace. The author focuses on the cyberwar qualifications, according to which such acts can be recognized as a crime of aggression.*

Keywords: *cyberwar, cybercrime, information and communication technologies, crime of aggression, principles of international law.*

Аннотация. *В статье исследуется вопрос международно-правовой квалификации кибервоен. Рассматривается соотношение понятий "кибератака", "кибернападение", "киберпреступление" и "кибервойна", на основании чего автор предлагает собственные дефиниции. Детально анализируются основания применения норм международного гуманитарного права и международного уголовного права касательно кибервоен. Исследуется проблема расширения сферы действия основных принципов международного права в киберпространстве. Автор акцентирует внимание на квалификационных признаках, согласно которым акты кибервойны могут быть признаны преступлением агрессии.*

Ключевые слова: *кибервойна, киберпреступность, информационно-коммуникационные технологии, преступление агрессии, основные принципы международного права.*

Постановка проблеми. Виходячи із основних принципів міжнародного права, зокрема мирного вирішення спорів та незастосування сили і погрози силою, а також цілей, проголошених Статутом ООН, міжнародне співтовариство зобов'язане вживати всіх необхідних засобів для запобігання та усунення загрози миру. Тому, одним з пріоритетів для міжнародного права є підтримання і захист миру, що неможливо без заборони та виключення війни як засобу ведення національної політики. За таких умов міжнародне нормотворення повинно вчасно реагувати на виклики сучасності, в тому числі на зародження тенденцій до виникнення нових асиметричних джерел сили, серед яких і кібернетичні можливості впливу [1, с. 10].

Резолюцією Генеральної Асамблеї ООН A/RES/55/29 від 11 грудня 2000 року "Роль науки і техніки в контексті міжнародної безпеки і роззброєння" міжнародне співтовариство висловило занепокоєння тим, що застосування науки і техніки можливе і у воєнних цілях, що може значною мірою сприяти удосконаленню та модернізації сучасних систем зброї, зокрема зброї масового знищення. Генеральна Асамблея ООН також з тривогою відзначала, що науково-технічні досягнення можуть бути використані з метою посилення гонки озброєнь, придушення національно-визвольних рухів та позбавлення окремих осіб і народів основних прав [2].

Як слушно зазначав, М. Тухачевський в "Питаннях сучасної стратегії" (1926 р.): "Відповісти на запитання – який характер буде мати уся майбутня війна – неможливо, бо мірою свого розвитку війна змінює свої форми, свій характер і передбачити їх заздалегідь неможливо" [3]. Таким чином, разом із розвитком суспільних відносин слід відзначити і трансформацію міжнародних спорів, які тепер вирішуються не типовими методами та засобами.

Екс-Президент США Обама стверджував, що: "Кіберзагрози можуть нашкодити навіть міжнародному миру і безпеці, оскільки традиційні форми конфлікту розширюються вже і на Інтернет" [4]. Хоча, міжнародне співтовариство неодноразово висловлювало занепокоєння тим, що новітні технології потенційно можуть використовуватися в цілях, несумісних із завданнями щодо забезпечення міжнародної стабільності та безпеки, і в змозі негативно впливати на цілісність інфраструктури держав, порушуючи їх безпеку як у цивільній, так і у військовій сферах (Туніська програма для інформаційного суспільства; Кодекс з захисту прав користувачів в кіберпросторі ЮНЕСКО; Резолюція ГА ООН A/HRC/20/L.13 від 29.06.2012 р.; Резолюції ГА ООН A/HRC/17/27 від 16.05.2011 р. тощо), станом на сьогоднішній день немає жодного міжнародно-правового акту, що містив би визначення "кібервійни" та забороняв її.

Результати аналізу наукових публікацій. Проблематика протидії кібервійнам є порівняно новою, але за рахунок її важливості неодноразово виділялась об'єктом наукових досліджень різних спрямувань. Серед зарубіжних авторів, що внесли значний вклад у розробку окресленої проблеми виділяємо: М. Кеттеманн (M. Kettemann), О. Хетавей (O.A. Hathaway), Дж. Андрес (J. Andress), С. Вінтерфілд (S. Winterfield), Дж. Валух (Jozef Valuch), О. Гамулак (Ondrej Hamulak). Серед вітчизняних фахівців з міжнародного права різні аспекти міжнародно-правової протидії інформаційним та кібернетичним війнам висвітлювали І.М. Забара, О.О. Мережко, А.В. Пазюк.

Найбільш ґрунтовним дослідженням сучасного міжнародного кримінального права є підручник за редакцією Герхарда Верле "Принципи міжнародного кримінального права". Слід відзначити також підрозділ "Злочинність у кіберпросторі: міжнародно-правовий дискурс" у підручнику "Теорія та практика міжнародного права" за редакцією професора Н.А. Зелінської, виданого у 2017 році.

Незважаючи на інтерес вчених до окремих аспектів проблеми протидії кібервійнам, питання міжнародно-правової кваліфікації кібернетичних актів досі залишається дискусійним.

Метою статті є комплексне дослідження міжнародно-правового регулювання застосування сили у кіберпросторі, а завданнями – визначення поняття та кваліфікаційних ознак кібервійни відповідно до норм сучасного міжнародного права.

Її новизна полягає в тому, що вперше у вітчизняній доктрині здійснено комплексне дослідження, в результаті якого надано авторський погляд на питання кваліфікації застосування сили у кіберпросторі як злочину за міжнародним правом.

Виклад основного матеріалу. Поняття “кібервійни” (cyberwar) не є новим, однак єдине узагальнене його визначення відсутнє. У доктрині та практиці міжнародного права паралельно застосовуються такі терміни як: “бойові дії у кіберпросторі” (cyberwarfare), “кібератака” (cyberattack), “кіберзлочинність” (cybercrime). Варто погодитись з автором статті “Коли кіберзлочин є актом кібервійни?” Тоні Бредлі (Tony Bradley), що існують значні відмінності у застосуванні термінів “кіберзлочинність”, “кібервійна”, “кібершпіонаж”, “кібер-хактивізм” та “кібертероризм”, що окрім теоретичної дискусії спричиняє ускладнення процесу визначення, який рівень правоохоронних органів необхідно застосовувати щодо конкретної атаки [5]. Дж. Андрес (J. Andress) і С. Вінтерфілд (S. Winterfield) також стверджують: “Визначити, що таке кібервійна, досить важко. Фактично, обидві дефініції – “кібер” і “війна” – є предметом дискусій” [6].

Ускладнює ситуацію безсистемне використання термінів “кібервійна”, “інформаційна війна”, “гібридна війна” засобами масової інформації як синонімів. Єдиних підходів до розуміння понять “інформаційна війна” та “гібридна війна”, так званих технологій “м’якої сили” сьогодні не існує. За допомогою них вчені часто пояснюють зміни у способах та веденні воєнних дій, які характеризуються поєднанням нетипових для класичного міжнародного права засобів, зокрема інформаційних. В умовах глобального інформаційного простору, з одного боку, весь світ має змогу слідкувати за “полем бою”, а з іншого – відбувається серйозне спотворення у висвітленні подій державами-учасниками конфлікту, в першу чергу, агресором. Однак, на нашу думку, ототожнення названих явищ з кібервійною є необґрунтованим, а їх аналіз виходить за рамки предмету представленого дослідження.

В основі розуміння феномену кібервійни, на наш погляд, лежить співвідношення понять – кібервійна, кібератака чи кібероперація, а також кіберзлочин. На практиці їх досить складно розрізнити, в тому числі відповідно кваліфікувати. Для вирішення термінологічної дискусії можна скористатись підходом, запропонованим Ендрю Стормсом (Andrew Storms), фахівцем з інформаційних технологій та безпеки. На його думку, при неможливості розмежування наведених вище понять, слід видалити префікс “кібер” і застосовувати ті ж рішення, які повинні бути використанні в класичному кримінальному праві [5]. Крім цього, як стверджує автор, важко уявити будь-який акт кібервійни, який також не буде порушенням чинних законів. У цьому сенсі кібервійна завжди є кіберзлочином, але не кожен кіберзлочин може бути визнаний актом кібервійни.

Український вчений О.О. Мережко зазначає, що у міжнародному праві немає чітких критеріїв, за допомогою яких можна було б відокремити акти звичайного комп’ютерного хуліганства від таких нападів, які завдяки своїй серйозності мають характер збройного нападу на державу, або є початком збройної агресії проти певної держави [7, с. 151].

Відповідно до норм сучасного міжнародного права, а саме Додаткового протоколу до Женевських конвенцій від 12.08.1949 року, що стосується захисту жертв міжнародних збройних конфліктів (Протокол І від 08.06.1977 року), в період збройних конфліктів нападами визначаються: “акти насильства щодо противника незалежно від того, здійснюються вони під час наступу чи оборони” (ст. 49) [8]. Названий протокол поширює свою дію на будь-які напади та об’єкти, незалежно від території, на якій вони здійснюються або розташовуються (на суші, у повітрі чи на морі). Звичайно, у 1977 р. кіберпростір ще не існував і не міг бути формально врахованим у положеннях зазначеної статті.

Виникає логічне питання, як можна кваліфікувати у міжнародному праві акти насильства, що здійснюють в кіберпросторі з метою наступу чи оборони. Відповідно до Таллінського посібника із застосування міжнародного права до кібервійни, опублікованого у 2013 році групою спеціалістів з міжнародного права на замовлення Спільного центру НАТО з обміну передовим досвідом у сфері кіберзахисту (NATO Cooperative Cyber Defence Centre of Excellence): "кібератака є кібероперацією, наступальною чи оборонною, внаслідок якої передбачається завдання шкоди або заподіяння смерті людям, пошкодження чи знищення об'єктів" [9]. Посібник, водночас, не має жодної юридичної сили і може використовуватися як довідниковий і рекомендаційний матеріал.

Джозеф Валух (Jozef Valuch) та Ондрей Гамулак (Ondrej Hamulak) в книзі "Застосування сили проти України та міжнародного права" стверджують, що не всі операції та дії в кіберпросторі можна кваліфікувати як кібератаки [10, с. 217-219] . При цьому автори не надають уточнюючого переліку чи класифікації відповідних кібероперацій. Згідно з Таллінським посібником "кібероперація являє собою застосування сили у випадку, коли її масштаб та наслідки можуть зрівнятись з не кіберопераціями, досягаючи рівня застосування сили" [9].

Однак, наведені визначення не дають змогу виділити всі необхідні кваліфікаційні ознаки кібернападу. Не визначаються, зокрема необхідні умови суб'єктного складу – хто та проти кого може їх здійснювати. Діяти у кіберпросторі мають змогу не лише окремі особи, групи осіб чи організації (у тому числі і терористичні), але й держави чи коаліції держав. Особливо вигідно "розмиваються" кордони між війною та миром. Фактично вчинені "кібернетичні атаки" можуть здійснюватися окремо або в поєднанні з іншими нападами та загрожувати суверенітету і безпеці держави. В рамках проведеного дослідження виділяємо три можливі суб'єктних складів кібернетичних нападів:

1) атака здійснюється фізичними або юридичними особами, їх об'єднаннями чи державами проти фізичних чи юридичних осіб або їх об'єднань;

2) атака здійснюється фізичними та юридичними особами, а також їх об'єднаннями самостійно чи за участі (сприяння, фінансування) держави проти держав чи міжнародного правопорядку;

3) атака здійснюється збройними силами або спеціальними підрозділами держави проти інших держав чи міжнародного правопорядку;

У першому та другому випадках матимуть місце факти вчинення кіберзлочинів. Наслідками таких атак може бути нанесення значної шкоди або навіть спричинення смерті людей, пошкодження чи знищення окремих об'єктів. В цьому контексті також важливо відзначити, що в результаті таких атаки можуть бути виведені із ладу навіть об'єкти критичної інфраструктури з масштабними і серйозними наслідки.

Разом із тим, особливого статусу набувають протиправні дії осіб, що підтримуються чи фінансуються державами. Прикладом такої атаки була загроза зловмисного програмного забезпечення Stuxnet, яке розроблено для того, щоб завдати шкоди фабриці зі збагачення урану в Ірані. Stuxnet був створений, щоб пошкодити фізичне обладнання, яке контролюється комп'ютерами. Він використовував програмні модулі, що були націлені на виконання певного завдання шкідливого програмного забезпечення. У Талліннському посібнику визначається, що кібератака з використанням шкідливого програмного забезпечення Stuxnet може бути визнана "озброєним нападом" [9]. Жертви таких атак мають право завдати удару у відповідь з метою самозахисту. Хакери, що беруть участь у конфлікті між державами, автоматично набувають статусу комбатантів.

У третьому випадку, коли атака здійснюється збройними силами або спеціальними підрозділами держави проти інших держав чи міжнародного правопорядку, на нашу думку, обґрунтовано буде говорити про міжнародний кібернетичний напад. А за умов системності таких атак – міжнародний кібернетичний конфлікт (cyberwarfare). Антонович П.І. у статті "Про сучасне розуміння терміну кібервійна", визначає кібернетичну війну як систематичну боротьбу в кіберпросторі між державами (групами держав), політичними групами, екстремістськими і терористичними та ін. угрупованнями, яка проводиться в формі атакуючих та оборонних дій [11, с. 90]. При чому, автор наголошує на системності такої боротьби, тобто цілісності, послідовності, єдності, підпорядкованості заданій меті дій агресора, які поєднуються з іншими діями. Стів Ренджер (Steve Ranger), надаючи визначення бойовим діям у кіберпросторі (cyberwarfare), вказує на ознаку розміру завданої шкоди: "це цифрова атака, яка є настільки серйозною, що може прирівнюватись до фізичної атаки" [12].

Отже, постає наступне дискусійне питання, чи може окремий кібернетичний напад бути визнаним кібервійною, за умови що він призводить до особливо значних негативних наслідків. Також чи можуть визнаватись кібернетичною війною систематичні кібернапади, що не призводять до тяжких наслідків, але здійснюються систематично і цілеспрямовано? Наприклад, DOS-атаки на комп'ютерні системи державних органів Естонії, що здійснювались протягом квітня 2007 року. Однак, ці питання також залишаються відкритими для наукової дискусії, зважаючи на відсутність міждержавного консенсусу.

Важливим в контексті проведеного дослідження є підхід запропонований колективом американських авторів в роботі "Право кібератак" щодо розмежування "кібератаки", "кіберзлочину" та "кібервійни" (cyberwarfare) [13]. В праці визначається, що на відміну від кіберзлочинів, які є порушеннями кримінального права з використанням комп'ютерних технологій і вчиняються недержавними суб'єктами, кібератаки здійснюються для виведення з ладу комп'ютерної мережі з політичних мотивів чи національної оборони. Натомість кібервійна, на думку авторів, є кібератакою, наслідки якої прирівнюються до "озброєного нападу" або здійснюються в умовах озброєного конфлікту. У публікації до кібератак відносяться три види діянь – DOS-атаки, поширення неправомірної інформації та проникнення в комп'ютерну систему, що перебуває під захистом. Однак, всі названі види відносяться до кіберзлочинів. У такому випадку, можна визначати будь-який кіберзлочин кібератакою за умови, що він здійснюється з мотивів політики чи національної оборони.

Міжнародне гуманітарне право та правила і звичаї ведення війни застосовуються під час озброєних конфліктів, як міжнародного, так і неміжнародного характеру. Апеляційна палата Міжнародного кримінального трибуналу по колишній Югославії надала наступне визначення озброєному конфлікту в своєму рішенні від 02.10.1995 року: "озброєний конфлікт відбувається у тих випадках, коли військова сила застосовується державами або коли здійснюється тривале військове насильство між урядами та організованими озброєними групами чи між такими групами всередині однієї держави" [14]. Виходячи із цього положення, на нашу думку, дія міжнародного гуманітарного права може поширюватись і на кібернетичні конфлікти за умови їхньої відповідності таким критеріям, як: 1) кібернетичні засоби впливу будуть кваліфікуватись як військова сила або військове насильство; 2) вони будуть здійснюватися державами або організованими озброєними групами.

Джозеф Валух (Jozef Valuch) та Ондрей Гамулак (Ondrej Hamulak) зазначають, що міжнародне право регулює "cyberwarfare" (бойові дії в кіберпросторі) відповідно до jus

ad bellum і jus in bello, однак через особливу специфіку кіберпростору окремі норми міжнародного права не можуть застосовуватись до нього vis-à-vis, зокрема щодо проблеми юрисдикції [10]. НАТО також повністю визнає дію міжнародного права та міжнародного гуманітарного права у кіберпросторі.

Матіас Кеттеманн (Matthias Kettemann) у статті "Посилення кібербезпеки за рахунок міжнародного права" стверджує, що норми Статуту ООН, які забороняють агресію та втручання є дійсними і для міжнародного права кібербезпеки [15]. За умови відсутності універсального договору щодо кібербезпеки цю сферу, на його думку, можна врегулювати лише на основі звичаїв та основних принципів міжнародного права.

Одним із фундаментальних принципів міжнародного права є принцип суверенної рівності держав, відповідно до якого кожна держава володіє юрисдикцією та владою в межах своєї території, а відповідно і інфраструктури інформаційно-комп'ютерних технологій (ІКТ), що розташована на ній. Саме названий принцип покладає на держави відповідальність забезпечити, щоб жодних атак проти інших країн чи інституцій, які б могли порушити міжнародне право, не було організовано чи здійснено з її території [15].

В справі Corfu Channel Міжнародний суд ООН визнав, що принцип добросусідства (ст. 74 Статуту ООН) означає також зобов'язання кожної держави не дозволяти використовувати власну територію для дій, що суперечать правам інших держав [16]. Принцип "не завдавати шкоди", що був застосований в справах Trail Smelter та Lac Lanoux, отримав нормативне закріплення в Стокгольмській декларації 1972 р., а також Ріо декларації 1992 р. та існує як звичаєва норма.

Особливого значення для регулювання кіберпростору і забезпечення кібербезпеки набув принцип due diligence (належна добросовісність), що широко застосовується для боротьби з тероризмом і фінансуванням тероризму [15]. Виходячи із названих принципів можна говорити про існування зобов'язання держав inter alia попереджати кібератаки, що готуються з їхньої території, та створювати правову систему забезпечення та сприяння кібербезпеці.

У монографії "Проблеми теорії міжнародного публічного та приватного права" О.О. Мережко пропонує проект Конвенції про заборону використання кібервійни в глобальній інформаційній мережі інформаційних і обчислювальних ресурсів (Інтернет). У ст. 1 проекту надається наступне визначення: "кібервійна – використання Інтернету й пов'язаних з ним технологічних та інформаційних засобів однією державою з метою заподіяння шкоди військовій, технологічній, економічній, політичній та інформаційній безпеці та суверенітету держави" [7, с. 152]. В проекті автор також пропонує визнати Інтернет загальною спадщиною людства, що підлягає використанню виключно в мирних цілях. Компанія Cisco також визначає кібервійну як Інтернет-конфлікт, який передбачає проникнення у комп'ютерні системи та мережі інших країн [17].

Вважаємо, дещо неточним звуження кібервійни лише щодо використання Інтернету. На нашу думку, кібернетична війна відбувається у кіберпросторі, що є однією із сутнісних ознак цього явища. Зокрема, рішення Сенату США, прийняте у 2009 році, офіційно проголошує кібернетичний простір новим середовищем (domain) ведення бойових дій та визначається доцільність його об'єднання з космічним простором в рамках виконання завдань на новому, "геоцентричному театрі воєнних дій" (Spherical Area of Operation).

В умовах неоднозначності застосування норм міжнародного права до кіберпростору держави здійснюють нарощування власних кібернетичних ресурсів. Так, окремі органи в сфері кібербезпеки створені в більшості держав світу (Франція, Великобританія, США, Німеччина, Російська Федерація, Україна та ін.). Як наслідок, на наш погляд, має місце нова стадія "гонки озброєнь". Тому окремо слід розглянути міжнародні норми, що можуть бути застосовані для регулювання засобів здійснення кібернападів чи атак – кібернетичної зброї.

ІКТ надають нові можливості для удосконалення вже існуючої зброї, а також створення нових її видів. В доктрині існують погляди про необхідність розробки міжнародної угоди про заборону окремих видів новітньої зброї. Формально така домовленість може бути прийнята як додатковий протокол до Конвенції про заборону або обмеження застосування конкретних видів звичайної зброї, які можуть вважатися такими, що завдають надмірних ушкоджень або мають невибіркову дію.

Міжнародне співтовариство активно здійснює дослідження в сфері новітніх озброєнь. Серед таких видів зброї, в першу чергу, слід відзначити бойові автономні роботизовані системи (БАРС), смертоносні автономні засобаи (САЗ), робототехнічні комплекси (РТК). Названі системи є прикладами автономної зброї, що може самостійно виявляти, ідентифікувати та вражати ціль за допомогою відповідних датчиків і штучного інтелекту . Хоча, використання автономних озброєних засобів передбачає існування віртуального простору, де знаходиться відповідне програмне забезпечення, здійснюються автоматизовані процеси, такі види зброї не можна вважати кібернетичними. Автономна зброя застосовуються в фізичному просторі (на суші, в повітрі, на морі).

На думку В. Каберник, кіберзброєю є найрізноманітніші технічні та програмні засоби, найчастіше спрямовані на експлуатацію вразливостей у системах передачі та обробки інформації або програмно-технічних системах (віруси типу Flame, зомбі-мережі, DOS і DDOS-атаки) [18]. П. Паганіні стверджує, що кіберзброя – це певний комп'ютерний код, який використовується або призначений для використання з метою загрози або заподіяння фізичної, функціональної або психічної шкоди структурам, системам або живим істотам [19].

Прикладом кіберзброї в більшості джерел визначається вірус Stuxnet, що описувався вище. Його особлива небезпечність полягає в тому, що він був першим вірусом, який наносив безпосередню фізичну шкоду комп'ютерним системам. Інформатизація та автоматизація багатьох процесів призвела сьогодні до широкого використання ІКТ на підприємствах, виробництві, всіх сферах промисловості, гідро- та атомних електростанціях, транспорті, в медицині тощо. А тому, як зазначає М. Камчатний, кіберзброя уже визначається летальною [20].

Застосування державою кібернетичної зброї, може розглядатись як міжнародний злочин агресії. Найбільш тяжкі міжнародні злочини – це такі міжнародні правопорушення, шо ставлять під загрозу знищення існуючого міжнародного порядку, порушують права та інтереси всього світового співтовариства, як правило вчиняються з неправомірним застосуванням збройних сил, інших неправомірних примусових заходів, ставлять під загрозу існування держави тощо [22, с. 114]. Хоча кібератаки не передбачають застосовування збройних сил у розумінні класичного міжнародного права, використання кібернетичної зброї може поставити під загрозу як національний, так і міжнародний правопорядок. Наприклад, застосування вірусів типу Stuxnet.

Діяння підпадають під дію міжнародного кримінального права, якщо воно відповідає трьом умовам: воно повинно тягнути за собою індивідуальну відповідальність та бути караним; норма, яка встановлює таку відповідальність повинна входити в систему міжнародного права; діяння повинно бути караним незалежно від того, чи включене воно в національне право чи ні [23, с. 38-39]. Злочинами за міжнародним правом є воєнні злочини, злочини проти людяності, геноцид і злочин агресії.

Як зазначається в колективному підручнику під редакцією Герхарда Верле "Принципи міжнародного кримінального права", злочин агресії перебуває "в стані невизначеності" [22, с. 39]. На думку авторів, безпосередньо за міжнародним звичаєвим правом криміналізується виключно агресивна війна (заборона війни передбачена низкою міжнародно-правових актів, серед яких Пакт Бріана-Келлога від 27 серпня 1928 року та Статут ООН). Зміст терміну "акт агресії", відповідно до ст. 39 Статуту ООН, конкретизовано Резолюцією ГА ООН 3314 (XXIX) від 14.12.1974 р., що визначає акт агресії як "застосування озброєної сили державою проти суверенітету, територіальної недоторканості чи політичної незалежності іншої держави" [23]. Злочин агресії охоплює акти меншої інтенсивності та масштабу, аніж війна [23, с. 38]. Як приклад актів агресії різні автори наводять: напад озброєних сил, блокада, надання підтримки озброєним бандам на територіях інших держав тощо. Більш детальний, хоча й невичерпний, перелік дій, що можуть бути кваліфіковані як акт агресії міститься в ст. 3 Резолюції ГА ООН 3314. Тоні Бредлі (Tony Bradley), наприклад, проводить паралель між військово-морською блокадою під час Кубинської ракетної кризи і атаки відмови в обслуговуванні (DOS-атакою) проти державної інфраструктури. За його переконанням, такі дії можуть бути бойовими і агресивними, фінансуватись державою, але не досягати значення "акту війни" [5].

На нашу думку, кібератаки за основними кваліфікаційними ознаками можуть прирівнюватись до дій, передбачених ст. 3b "бомбардування озброєними силами держави території іншої держави або застосування будь-якої зброї державою проти території іншої держави" [24]. Формулювання "застосування будь-якої зброї" може включати в себе розуміння "застосування кіберзброї". З іншої сторони, об'єкт злочину агресії – "проти території іншої держави" опосередковано відноситься до екстериторіального кібернетичного простору.

Для того, щоб кібервійна була кваліфікована за міжнародним правом як злочин агресії, необхідно щоб такі дії відповідали всім елементам, відповідно до Додатку II "Поправки до елементів злочинів" до Римського статуту Міжнародного кримінального суду. Оцінити ступінь порушення кібернетичними атаками Статуту ООН можна відповідно до п. 6 та 7 Додатку III "Положення про розуміння щодо поправок до Римського статуту Міжнародного кримінального суду, стосовно злочину агресії". Так, визначається обов'язковість розгляду всіх обставин кожного конкретного випадку, включаючи тяжкість відповідних актів та їх наслідки, оскільки агресія визнається найбільш серйозною і небезпечною формою незаконного застосування сили. З іншої сторони, встановлюється необхідність наявності трьох компонентів при кваліфікації факту агресії як порушення Статуту ООН: характеру, тяжкості і масштабу. Названі ознаки повинні існувати одночасно, внаслідок чого злочин можна визнати "явним" [24].

Слід наголосити на тому, що аналізоване визначення злочину агресії схвалене Резолюцією ГА ООН № 3314, має характер soft law і потребує конвенційного закріплення. Як стверджує К.А. Важна, наявність факту перетворення положень названої резолюції на звичаєві норми на сучасному етапі є дискусійним [25, с. 92].

Висновки.

Кібервійна – це значні, масштабні, цілеспрямовані та систематичні кібератаки із застосуванням кіберзброї, здійснювані збройними силами та/або спеціальними підрозділами держави проти суверенітету, територіальної цілісності, незалежності іншої держави та міжнародного миру і стабільності.

Кібератака – порушення прав і законних інтересів учасників кіберпростору за допомогою ІКТ, що здійснюються фізичними та юридичними особами за участі (сприяння, фінансування тощо) держав з політичних мотивів. Кібератаки, що фінансуються державами, але за своїм характером не є значними, масштабними та систематичними, не можуть визнаватись кібервійною. Їх можна кваліфікувати як недружні акти.

За умови, якщо кібератака включає здійснення дій, передбачених кримінальним і міжнародним правом, такі діяння можуть бути кваліфіковані як кіберзлочини та міжнародні кібернетичні злочини відповідно.

Норми сучасного міжнародного права, зокрема основні принципи міжнародного права є чинними і для кіберпростору. Це означає, існування заборони здійснювати акти агресії у кіберпросторі на підставі принципів суверенної рівності держав, незастосування сили і погрози силою, невтручання у внутрішні справи, а також спеціальних принципів – добросусідства і due diligence.

Відсутність формально вираженого консенсусу держав та доктринальна невизначеність з питання кваліфікації кібервійни за міжнародним правом залишає його відкритим для дискусії. В таких умовах відбувається процес поглиблення інформаційного протистояння між державами, мілітаризації кіберпростору, розробки кіберзброї, та нарощування кібернетичних потужностей і тактик як національного ресурсу держав. В позитивному праві не існує достатніх запобіжних засобів для захисту слабкої сторони в умовах застосування інформаційних методів впливу. А отже, єдиним виходом для держав є захист і здійснення кібернетичних атак у відповідь.

В сучасній доктрині та практиці міжнародного права існують два можливі підходи до кваліфікації кібернападів, що складають кібервійну. З однієї сторони, на них може поширюватись дія міжнародного гуманітарного права за умови їхньої відповідності таким критеріям, як: 1) кібернетичні засоби впливу будуть кваліфікуватись як військова сила або військове насильство; 2) вони будуть здійснюватися державами або організованими озброєними групами. В рамках віртуального простору розмиваються не лише кордони, а й різниця між воєнними цілями і мирними об’єктами (серед яких і культурні цінності, об’єкти критичної інфраструктури та ін.), між військовим та цивільним населенням. З іншої сторони, кібератаки можна кваліфікувати як злочин агресії за міжнародним кримінальним правом. Таке рішення повинно розглядатись в кожному конкретному випадку, оцінюючи характер, тяжкість і масштаб порушення Статуту ООН. Найбільш обґрунтованим вважаємо визнання кібервійни як акту застосування сили відповідно до Статуту ООН, а в окремих випадках – злочину агресії.

Використана література

1. Антипенко В.Ф. Проблеми ефективності міжнародного права. *Проблеми ефективності міжнародного права*: матер. тез. міжн. наук.-практ. конф., м. Київ, 29 бер. 2013 р. Київ, 2013. С. 9-11.

2. Про використання науково-технічного прогресу в інтересах світу і на благо людства: Декларація ГА ООН від 09 грудня.1975 р. URL: https://undocs.org/ru/A/RES/3384(XXX)

3. Требін М. П. “Гібридна” війна як нова українська реальність. *Український соціум.* 2014. URL: http://nbuv.gov.ua/UJRN/Usoc_2014_3_13

4. International Strategy for Cyberspace, 2011. URL: https://obamawhitehouse.archives.gov /sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

5. Bradley T. When is a Cybercrime an Act of Cyberwar? URL: https://www.pcworld.com/ article/250308/when_is_a_cybercrime_an_act_of_cyberwar_html

6. Andress J., Winterfeld S. Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners. URL: http://index-of.es/Hack/Cyber%20Warfare.pdf

7. Мережко О.О. Проблеми теорії міжнародного публічного і приватного права. Київ: Юстиниан, 2010. 320 с.

8. Додатковий протокол до Женевських конвенцій від 12.08.1949 р., що стосується захисту жертв міжнародних збройних конфліктів (Протокол I від 08.06.1977 р.). URL: http://zakon.rada.gov.ua/laws/show/995_199

9. The Tallin Manual on International Law applicable to Cyber Warfare Prepared by International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. URL: http://csef.ru/media/articles/3990/3990.pdf

10. Sayapin S., Tsybulenko E. The use of force against Ukraine and International Law. *Springer*. Netherlands, 2018. 465 p.

11. Антонович П.И. О современном понимании термина “кибервойна”. *Вестник академии военных наук*. 2011. № 2(35). С. 89-96

12. Ranger S. What is cyberwar? Everything you need to know about the frightening future of digital conflict. URL: https://www.zdnet.com/article/cyberwar-a-guide-to-the-frightening-future-of-on line-onflict

13. Hathaway O.A. The Law of Cyber-attack. URL: https://law.yale.edu/system/files/doc uments/ pdf/cglc/LawOfCyberAttack.pdf

14. United Nations International Criminal Tribunal for the former Yugoslavia. URL: http://www.icty.org/case/tadic/4

15. Matthias C. Kettemann. Ensuring Cybersecurity through International Law. URL:https://www. jstor.org/stable/26296737?read-now=1&refreqid=excelsior%3A6fb9e65c043f51fa573028c4c61c9e93 &seq=4#page_scan_tab_contents

16. Summary of relevant aspects of Corfu Channel case (Merits). URL: https://www.iilj.org/wp-content/uploads/2016/08/Summary-of-and-extract-from-Corfu-Channel-Case-United-Kingdom-v-Alb ania.pdf

17. Cisco. Що таке кібервійна? URL: https://static-course-assets.s3.amazonaws.com/Cyber Sec2/uk/index. html#1.4.1.1

18. Каберник В. В. Центр военно-политических исследований. *Кибервойна и кибероружие*. URL: http://eurasian-defence.ru/?q=node/3115

19. Pierluigi Paganini. Cyber Weapons. April 3, 2012. URL:http://securityaffairs.co/wordpress/ 3896/intelligence/cyber-weapons.html

20. Камчатний М. Заборонені засоби ведення кібервійни. URL: http://pgp-journal.kiev.ua/ archive/2017/9/44.pdf

21. Задорожній О.В., Буткевич В.Г., Мицик В.В. Конспект лекцій з основ теорії міжнародного права. Київ: Либідь. 2001. С. 114-115.

22. Верле Герхард. Принципы международного уголовного права: учебник / пер. с англ. С. В. Саяпина. Одеса: Фенікс; Москва: ТрансЛит, 2011. 910 с. С. 38-39.

23. Определение агрессии: утверждено резолюцией 3314 (XXIX) Генеральной Ассамблеи ООН от 14 декабря 1974 года URL: http://www.un.org/ru/documents/decl_conv/conventions/aggres sion. shtml

24. Резолюція RC/Res.6: прийнята консенсусом на 13-му пленарному засіданні 11 червня 2010 р. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=50984&pf35401 =301758

25. Важна К.А. Визначення агресії у сучасному міжнародному праві: матеріали наук.-практ. конф. *Україна і світ,* м. Київ, 19 квіт. 2016 р. *Україна і світ:* науковий журнал (Факультет журналістики і міжнародних відносин Київського національного університету культури і мистецтв). Київ: КНУКіМ, 2016. Вип. 1. С. 84-92.

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

УДК 340.132+316.324.8

УХАНОВА Н.С., старший науковий співробітник НДІІП НАПрН України

ВИКЛИКИ І ЗАГРОЗИ ПРАВАМ ТА БЕЗПЕЦІ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Анотація. *У статті проаналізовано вплив загроз інформаційній безпеці. У цьому контексті Доктрина інформаційної безпеки України одним із пріоритетів державної політики в інформаційній сфері визначає розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист. Охарактеризовано принципи забезпечення прав людини в умовах розвитку інформаційного суспільства. Досліджено світовий досвід дотримання прав людини у контексті розвитку інформаційних технологій. Підкреслено переважне значення принципу пропорційності, як однієї з найважливіших гарантій забезпечення прав людини при забезпеченні національної безпеки та інформаційної безпеки держави.*

Ключові слова: *загрози інформаційній безпеці, інформаційна сфера, інформаційні ресурси, інформаційно-телекомунікаційні технології, Доктрина інформаційної безпеки, права і свободи людини і громадянина.*

Summary*. The article analyzes the impact of threats to information security on human rights. In this context, the Doctrine of Information Security of Ukraine,determines the development of legal instruments for the protection of human rights and citizen's free access to information, its dissemination, processing, storage and protection as one of the priorities of the state policy in the information sphere. The principles of ensuring human rights in the conditions of the information societydevelopmentare characterized. The world experience in observing human rights in the context of the development of information technologies has been researched.The overriding importance of the principle of proportionality is emphasized as one of the most important guarantees of ensuring human rights while ensuring the national security and information security of the state.*

Keywords: *threats to information security, information sphere, information resources, information and telecommunication technologies, Doctrine of information security, rights and freedoms of humanand citizen.*

Аннотация. *В статье проанализировано влияние угроз информационной безопасности на права человека. В этом контексте Доктрина информационной безопасности Украины одним из приоритетов государственной политики в информационной сфере определяет развитие правовых инструментов защиты прав человека и гражданина на свободный доступ к информации, ее распространение, обработки, хранения и защиту. Охарактеризованы принципы обеспечения прав человека в условиях развития информационного общества. Исследован мировой опыт соблюдения прав человека в контексте развития информационных технологий. Подчеркнуто преимущественное значение принципа пропорциональности, как одной из важнейших гарантий соблюдения прав человека при обеспечении национальной безопасности и информационной безопасности государства.*

Ключевые слова: *угрозы информационной безопасности, информационная сфера, информационные ресурсы, информационно-телекоммуникационные технологии, Доктрина информационной безопасности, права и свободы человека и гражданина.*

Постановка проблеми. Вільне та безпечне існування особи, суспільства, держави та їх взаємодія залежить від захищеності інформаційної сфери від зовнішніх і внутрішніх загроз. Зокрема, у Доктрині інформаційної безпеки України забезпечення і захист прав людини відносяться до основного напрямку реалізації національних інтересів в інформаційній сфері.

Сучасний стан реалізації прав людини в інформаційній сфері пов'язаний з викликами, обумовленими застосуванням інформаційно-комунікаційних технологій (далі – ІКТ). Розвиток ІКТ призводить до розширення можливостей їх недобросовісного використання, яке створює загрози інформаційній безпеці і може призводити до порушень прав людини. У зв'язку з цим виникає проблема співвідношення інформаційної безпеки і прав людини. Шляхи вирішення означеної проблеми полягають насамперед у необхідності виявлення викликів і загроз правам та безпеці людини в інформаційній сфері, що нині є проблемою надзвичайно актуальною, оскільки Україна, як і всі цивілізовані країни світу, стала на шлях розвитку інформаційного суспільства.

Результати аналізу наукових публікацій. Правові аспекти впливу інформаційних і комунікаційних технологій на розвиток сучасного суспільства знайшли своє відображення в роботах О.А. Баранова, В.М. Брижка, О.Д. Довганя, Г.М. Линника, О.В. Олійника В.Г. Пилипчука, В.Б. Толубка, Є.Л. Ющука та інших дослідників. Розуміння інформаційної безпеки, на нашу думку, має ґрунтуватись на її визначенні з точки зору стану захищеності національних інтересів України в інформаційній сфері, що складається із сукупності збалансованих інтересів особи, суспільства і держави від внутрішніх та зовнішніх загроз. У науковій літературі наводяться подібні судження. Наприклад, О.В. Олійник сформулював теоретичне підґрунтя для подальшої системної характеристики напрямів та ієрархії безпекогенних чинників "ризик", "загроза", "виклик", "небезпека" [6, с. 6]. У той же час науковець справедливо вказує на принципові недоліки цього документу, адже Доктрина, на його думку, не визначає важливі аспекти забезпечення інформаційної безпеки України [6, с. 10]. Крім того, не менш важливим зауваженням щодо змісту зазначеного документу є відсутність принципу дотримання прав людини під час забезпечення інформаційної безпеки. Внесення цього доповнення слугуватиме надійним фундаментом в процесі формування державної політики, що стосується захисту прав людини.

Г.М. Линник обґрунтовано наголошує на наявності потенційних і реальних загроз в інформаційній сфері, які негативно впливають на суспільний розвиток держави та реалізацію її євроінтеграційних прагнень [7, с. 4]. У той же час, авторське розуміння інформаційної безпеки, як "діяльності суб'єктів права щодо задоволення національних інтересів в інформаційній сфері, шляхом управління реальними чи потенційними загрозами", має дискусійний характер, оскільки головний акцент у визначенні способів протидії реальним та потенційним загрозам інформаційній безпеці акцентований на управлінні ними [7, с. 7]. Вчений наводить ґрунтовну періодизацію становлення та розвитку інституту забезпечення інформаційної безпеки. В процесі її формування доходить висновку, що головним недоліком попередніх етапів функціонування системи забезпечення інформаційної безпеки є її недостатня орієнтація на дотримання прав і свобод людини і громадянина.

Є.Л. Ющук, розкриваючи ключові питання забезпечення інформаційної безпеки в мережі Інтернет, справедливо наголошує на всеохоплюючому впливі Інтернет-ресурсів, неможливості забезпечення захисту інформації, причому зазначений вплив, на думку автора, дуже часто має негативний характер [8, с. 5].

В.Б. Толубко розглядає інформаційні ресурси як ефективну зброю, яка використовується конфліктуючими сторонами на міждержавному рівні в процесі вирішення різноманітних конфліктів. Зокрема, вчений класифікує інформаційну зброю "за метою застосування; за об'єктами впливу; за механізмами реалізації впливу; за характером впливу на інформацію та інформаційні процеси; за масштабом вирішуваних завдань; за терміном дії тощо" [9, с. 18]. Окреслені автором завдання та напрями

забезпечення інформаційної безпеки у воєнній сфері мають безсумнівну наукову цінність та чинять безпосередній вплив на дотримання прав і свобод людини.

Заслуговує на увагу позиція О.Д. Довганя, який розглядає об'єкт організації національної інформаційної безпеки через призму трьох її складових компонентів: "основоположної суверенної інформації, національного інформаційного простору використання інформації та інформаційного виробництва" [10, с. 112]. Важливим є висновок автора щодо обов'язкової адекватності структурної організації системи управління інформаційною безпекою загальній системі державного управління.

Системні проблеми захисту приватності, у тому числі пов'язані з використанням новітніх ІКТ, розглядаються у низці праць В.М. Брижка та В.Г. Пилипчука [11, с. 60-70; 12, с. 16-37]. У роботах цих вчених є важлива ідея необхідності *формування інституту "права приватної власності людини на свої персональні дані", як основної складової загальної системи визначення захисту її прав,* яку можна розглядати як новацію в юридичній сфері. В умовах активного розвитку та поширення ІКТ типу Інтернет речей, Хмарних технологій, Великих Даних та їх конвергенції все складніше стає здійснювати захист персональних даних завдяки звичайних юридичних приписів. Сьогодні різноманітні ІКТ, кожна з яких на початку створення передбачала конкретне функціонально-цільове призначення, застосовують можливості інших ІКТ, які інтегруючись стали доповнювати одна одну і у комплексі створювати, так би мовити, надсумарний ефект конвергентності та надавати нову якість результатів від сумісного їх використання, що позначається на умовах реальних можливостей захисту прав людини в сфері персональних даних.

У контексті вищезазначеного, в роботі [13] доволі ґрунтовно розглядаються проблеми застосування сучасної інформаційної зброї в інформаційних війнах, зокрема в Інтернет. Визначено види, зміст, зброя, засоби нападу та захисту. Здійснено аналіз та систематизація наукових досягнень щодо розв'язування деяких техніко-технологічних і правових питань із захисту інформаційних ресурсів та знань, зокрема стосовно створення дієвих умов захисту персональних даних людини.

Метою статті є аналіз проблемних питань сучасного розвитку інформаційного суспільства, виявлення викликів і загроз правам та безпеці людини в інформаційній сфері та окреслення напрямів удосконалення національного законодавства у сфері інформаційної безпеки особи.

Виклад основного матеріалу. Постановка проблеми правового забезпечення інформаційної безпеки особи пов'язана, на нашу думку, перш за все з умовами формування стану її захищеності від внутрішніх і зовнішніх загроз у глобальному інформаційному суспільстві. Під викликами і загрозами інформаційній безпеці особи ми розуміємо актуалізовані та потенційні дії, події, процеси та явища, які чинять деструктивний вплив на психіку і свідомість людини та призводять до завдання шкоди її інтересам в умовах глобального інформаційного суспільства. До сучасних викликів і загроз інформаційній безпеці, на наш погляд, слід віднести:

1) загрози, які переслідують цілі: а) впливу на свідомість людини, на її психологічний стан, на формування екстремістських настроїв серед молоді; б) чинення деструктивного впливу, який шкодить здоров'ю людини (наприклад шляхом поширення заборонених до обігу лікарських засобів, тощо); в) оволодіння особистою інформацією, у тому числі з метою її використання у протиправних цілях; г) поширення ідеології тероризму, радикальних ідей в мережі Інтернет; д) вплив на статеву недоторканність та статеву свободу людини; е) фінансове шахрайство; є) розвиток антигромадських стереотипів поведінки, тощо;

2) навмисне поширення інформації обмеженого доступу, інформації, поширення або подання якої заборонено в Україні. Це: а) матеріали з порнографічним зображенням неповнолітніх та (або) оголошення про притягнення неповнолітніх в якості виконавців та учасників видовищних заходів порнографічного характеру; б) інформація про засоби розробки, виготовлення і використання наркотичних засобів, психотропних речовин та їх придбання, способи і місця культивування нарковмісних рослин; інформація про способи вчинення самогубства, а також заклики до вчинення самогубства;

3) загрози в мережі Інтернет: фішингові сайти, шкідливе програмне забезпечення, спам-розсилки, шахрайські сайти, рекламовані з метою отримання прибутку (фінансові піраміди, фальшиві Інтернет-магазини та ін.), Інтернет-майданчики, що впливають на індивідуальну свідомість молоді (веб-сайти, які сприяють поширенню кіберсуїциду, порносайти, чати і форуми які використовуються педофілами та сексуальними маніяками).

4) загрози, спрямовані на трафік віртуальної валюти Bitcoin, загрози конфіденційності персональних даних внаслідок ІКТ он-лайн-реклами Real-TimeBidding (RTB), загрози, які надходять від спеціальних файлів "кукі" (від англ. – cookie).

Як ключові принципи формування державної політики в галузі забезпечення інформаційної безпеки людини можуть бути прийняті: принцип визнання особи як ключового і найбільш уразливого учасника інформаційних відносин, відповідальності держави в інформаційній сфері, відповідності вживання організаційно-правових заходів безпеки реальним викликам і загрозам, а також принцип контролю за забезпеченням інформаційної безпеки людини, в тому числі за рахунок механізму захисту інформаційних прав і свобод громадськими організаціями. З метою реалізації принципу недоторканності приватного життя, неприпустимості збору, зберігання, використання і поширення інформації про приватне життя особи без її згоди, доцільно введення такого механізму, як моніторинг стану захищеності людини від внутрішніх і зовнішніх загроз в інформаційній сфері.

Ключове місце у забезпеченні прав і безпеки людини в інформаційній сфері належить захисту персональних даних. У зарубіжних країнах захист персональних даних заснований на загальних принципах роботи з ними: персональні дані мають збиратися і оброблятися тільки відповідно до закону та наділеними відповідними повноваженнями органами; персональні дані повинні бути адекватними заздалегідь визначеним цілям і розпорядження ними повинно обмежуватися за термінами, відповідним зазначеним цілям; бути точними і оброблятися тільки за згодою суб'єктів цих даних; персональні дані повинні бути доступні суб'єктам цих даних, в тому числі і для внесення в них уточнення; персональні дані повинні бути належним чином захищені.

У Грузії 1 березня 2017 року завершився тривалий процес розробки і прийняття поправок до Закону "Про електронні комунікації" від 20.11.13 р. № 1591. Рішення складного завдання дотримання прав людини і забезпечення безпеки країни завершилося прийняттям норм про створення спеціалізованого оперативно-технічного агентства, яке на підставі оперативної інформації про загрозу безпеці державі буде таємно прослуховувати і записувати телефонні розмови, а також контролювати соціальні мережі, здійснювати приховані відеозйомки, перевіряти поштові посилки [14]. За задумом авторів прийнятого парламентом Грузії закону, новий державний суб'єкт буде працювати за такою схемою: коли спецслужбам знадобиться інформація про громадян особистого характеру, вони спочатку запитають ордер в суді (як визначено законом і зараз), потім нададуть його новому державному відомству, а не провайдерам. Коротко кажучи, правозахисники хочуть, щоб доступ до "чорних скриньок" мали не

спецслужби, а нова структура. Юрист Центру вивчення і моніторингу за правами людини Г. Імнадзе – один з авторів поправок. Ідею створення окремої самостійної структури він назвав know-how грузинських правозахисників: *"Такого досвіду немає у інших країн – це наше know-how. Але у них і не було такого минулого, як у нас. Європейську модель ми не пропонуємо, тому що у нас інша ситуація – у нас провайдери могли знати, які саме дані запитують спецслужби. А це могло відбитися на безпеці країни. Вважаємо, що в Грузії право доступу і обробки особистої інформації має перейти до незалежної державної структури"* [15].

У правовій доктрині США визначення "інформаційна безпека" та "приватність" деталізується через перерахування конкретних елементів інформаційної сфери, на захист яких вона спрямована [16, с. 17]. Правові принципи конфіденційності, цілісності та доступності інформації виступають головною підставою визначення зазначених елементів. Так, при дотриманні принципу конфіденційності ознайомлення з конфіденційною інформацією, її обробка і пред'явлення вимоги про її надання допускаються тільки для особи, яка має право доступу до такої інформації. Роль принципу конфіденційності полягає у запобіганні шкоди, яку може бути заподіяно суспільним відносинам в результаті неправомірного надання та поширення інформації, що зберігається в таємниці в силу її значення для безпеки особи, суспільства та держави. Даному принципу відповідає свого роду право "зберігати у таємниці" інформацію, обмежувати доступ третіх осіб до неї, контролювати її цільове використання тощо.

На відміну від конфіденційності інформації, забезпечення її цілісності, набуло актуальності в процесі розвитку ІКТ та виникнення можливостей несанкціонованого доступу до неї з метою внесення змін або її знищення. Особа, яка володіє інформацією або правом доступу до інформації, має право вимагати забезпечення її цілісності, а також в ряді випадків цілісності носія інформації, тобто збереження їх в оригінальному, незмінному вигляді, забезпечення невтручання в структуру (форму) і зміст інформації. Зазначений принцип спрямований на забезпечення достовірності інформації, яка дозволяє зберігати між учасниками суспільних відносин необхідний рівень довіри і впевненості в тому, що вони мають справу з оригінальною інформацією та її джерелом.

Принцип доступності відіграє важливу роль у формуванні гарантій права людини на доступ до інформації. Вказаний принцип спрямований на запобігання обмеження і створення умов доступу до соціально-значимої інформації, перш за все під час взаємодії людини з органами влади, а також до іншої інформації, надання якої вона має право вимагати. Цей принцип лежить в основі реалізації заходів щодо забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування, екологічної інформації, в тому числі шляхом розміщення інформації на офіційних сайтах органів і організацій.

В свою чергу Доктрина інформаційної безпеки України одним із пріоритетів державної політики в інформаційній сфері визначає розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист [17]. Крім того, доступ до публічної інформації, відповідно до статті 4 Закону України "Про доступ до публічної інформації", здійснюється на принципах: прозорості та відкритості діяльності суб'єктів владних повноважень; вільного отримання, поширення та будь-якого іншого використання інформації, що була надана або оприлюднена відповідно до Закону, крім обмежень, встановлених законом; рівноправності, незалежно від ознак раси, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, мовних або інших ознак [18]. Зміст цих положень яскраво

демонструє, що допустимі згідно з Конституцією України [19] та міжнародними документами про права людини обмеження повинні відповідати за змістом та обсягом цілям обмежень, що вводяться, і можуть застосовуватися тільки для захисту інших рівнозначних правових цінностей.

На додаток до принципів конфіденційності, цілісності і доступності, в правовій доктрині вироблені спеціальні правові принципи захисту права на недоторканність приватного життя, в яких визначаються межі й умови здійснення даного права. У зв'язку з принципом конфіденційності такі спеціальні правові принципи визначають можливість збору персональних даних лише законними засобами і для конкретно визначених цілей за умови попереднього повідомлення або попередньої згоди суб'єкта персональних даних, забезпечення їх захисту від таких ризиків як втрата або несанкціонований доступ, знищення, використання, зміна або розкриття даних. Поряд з принципом цілісності застосовується принцип, при дотриманні якого персональні дані повинні відповідати цілям їх використання і відповідно до таких цілей мають бути точними, повними й актуальними. Принцип доступності доповнюється принципами, які створюють умови для доступу суб'єкта персональних даних до інформації про наявність у оператора і характер оброблюваних ним персональних даних такого суб'єкта, основні цілі їх використання, місце знаходження оператора, а також наділяють суб'єктів персональних даних додатковими правами, включаючи можливість знищення, виправлення, доповнення або зміни своїх персональних даних. Зазначені принципи наразі відображені в багатьох міжнародних актах, початок визначення яких було надано Конвенцією Ради Європи "Про захист осіб у зв'язку з автоматизованою обробкою персональних даних" від 28 січня 1981 року № 108 [20].

Конфіденційність особистої інформації забезпечується шляхом надання доступу або можливості збору і обробки такої інформації тільки тим особам, які отримали відповідну згоду її власника. Якщо доступ або можливості збору і обробки надаються на підставі закону, то обов'язковим є повідомлення власника про обробку персональних даних. Повідомлення також обов'язково при інших випадках, визначених суб'єктом персональних даних або встановлених законодавством, наприклад, при порушенні конфіденційності або цілісності персональних даних. Зазначені механізми надають суб'єкту персональних даних правові можливості контролю за їх використанням і, відповідно, гарантії недоторканності його приватного життя.

Зазначимо, що з розвитком мережі Інтернет та Інтернет-сервісів, створенням потужних колекцій інформації, вказані механізми виявляються недостатніми для дотримання права людини на недоторканність приватного життя. Фактично користувач поступово втрачає контроль над використанням та поширенням персональних даних про себе. Так, при використанні Хмарних технологій процес передачі та обробки даних стає для користувача невизначеним і на практиці може полягати у клонуванні інформації та її розміщенні на серверах, розташованих в різних національних юрисдикціях. Крім того, більшість користувачів дає згоду на обробку їх персональних даних, належним чином не ознайомившись з її умовами, не розуміючи правових наслідків такої згоди і не передбачаючи подальшого використання своєї особистої інформації. В результаті механізм надання згоди користувача на обробку його особистої інформації виявляється недосконалим та неефективним, а відтак, не забезпечує конфіденційності особистої інформації і реального захисту права на недоторканність приватного життя.

Для сучасної електронної комерції попередня згода і подальше повідомлення суб'єкта персональних даних можуть інколи створювати перешкоди розвитку бізнесу та впровадження інновацій. У зв'язку з цим обмеження свободи підприємницької

діяльності в Інтернеті, зумовлені використанням традиційних механізмів захисту права на недоторканність приватного життя, стають надлишковими.

Розвиток гарантій даного права здійснюється шляхом створення додаткових по відношенню до згоди суб'єкта персональних даних та його повідомлення механізмів захисту конфіденційності, які виражені в пред'явленні специфічних вимог до осіб, які здійснюють збір і обробку особистої інформації. Такі вимоги можуть полягати у встановленні спеціального правового режиму так званих чутливих даних, обмеження збору певної особистої інформації в цифровій формі, в тому числі геолокаційних і біометричних даних, обмеження автоматичного прийняття юридично значущих рішень. Формою правового захисту персональних даних також є обмеження їх передачі в національні юрисдикції, де не забезпечуються необхідні гарантії права на недоторканність приватного життя. Одночасно зростають вимоги до технічного захисту персональних даних для запобігання несанкціонованого доступу до них, усунення наслідків їх розкриття або компрометації.

У Європейському Союзі право на недоторканність приватного життя розглядається як фундаментальне право. Його захист гарантується ст. 8 Європейської Конвенції про захист прав людини і основоположних свобод 1950 року [21] і конституціями держав-членів ЄС. Пріоритет повного контролю особи щодо своїх персональних даних перед традиційними демократичними свободами (свободою підприємницької діяльності та свободою слова) лежить в основі кількох поколінь національних законів у сфері захисту недоторканності приватного життя, нормативних правових актів ЄС та рішень Європейського суду з прав людини, див., зокрема [22; 23].

На відміну від ЄС, в США спеціальні вимоги в сфері обробки персональних даних встановлені тільки в найбільш чутливих сферах. В інших сферах держава віддає пріоритет саморегулюванню, в основі якого знаходиться свобода підприємницької діяльності, свобода договору, свобода слова та друку. Держава впливає на суспільні відносини шляхом видання різного роду рекомендацій та політичних заяв.

В час бурхливого розвитку науково-технічного прогресу і стрімкого зростання цифрової економіки європейські законодавці проходять нову важливу віху в регулюванні захисту персональних даних. Європейський Парламент і Рада 27 квітня 2016 року прийняли Регламент (ЄС) 2016/679 "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 (Загальні Положення про захист даних)" [24 – 27]. Цей Регламент покликаний уніфікувати норми в європейських країнах щодо захисту персональних даних громадян ЄС і забезпечити їх надійніший захист. Нові правила стали відповіддю на громадське занепокоєння щодо стану справ захисту прав на приватність.

Метою Регламенту (ЄС) 2016/679 є:

- гармонізація законодавства про захист даних по всьому ЄС;
- модернізація законів про захист даних у світлі технологічних змін;
- посилення прав громадян;
- збільшення вимог до відповідальності й обов'язків контролерів даних та обробників даних;
- вдосконалення процесу створення облікових записів користувачів, а також контроль за дотриманням законів про захист даних;
- забезпечення більшої прозорості того, як використовуються дані, ким і для чого.

Регламент (ЄС) 2016/679 застосовується до компаній (незалежно від їхнього членства в ЄС), які обробляють особисті дані осіб, що проживають у ЄС, включаючи особисті дані клієнтів Global Logic, а також їх кінцевих замовників та працівників.

Згідно з Регламентом (ЄС) 2016/679, не можна просто так взяти і використовувати персональну інформацію, прикриваючись чекмарком на згоду про конфіденційність. Для цього необхідний, щонайменше реальний дозвіл суб'єкта даних і прозорий для нього механізм використання даних компанією. Компаніям, які мають справу з обробкою персональних даних, – а це всі компанії, що мають справу з кінцевим споживачем, доведеться облікувати все, починаючи з дати, коли клієнт надав чи відредагував інформацію, і закінчуючи тим, коли дані будуть видалені зі сховищ. І найголовніше, на запит власника потрібно буде в повному обсязі і в зрозумілій формі надавати йому всі ці дані, а також видаляти їх зі сховища за його бажанням.

За запитом користувачів, Інтернет-компанії зобов'язані, зокрема, надати інформацію, з якою метою використовуються персональні дані, чи не передані вони до третіх країн і т.д. Якщо компанія, наприклад, передає персональну інформацію до іншої країни, не маючи законних підстав для цього (в регламенті вони також указані) то штраф за такі дії буде ще більшим.

На нашу думку, багато людей досить безтурботно ставляться до своїх персональних даних. Особливо це небезпечно в авторитарних державах, що використовують Інтернет як засіб контролю над громадянами (приклад Китаю). Однак і в демократичних державах Європи використання зайвої інформації, викладеної в Інтернеті, може мати негативні наслідки.

У кращому випадку користувач отримує величезну кількість непотрібної реклами, в гіршому, вся інформація про нього, включаючи сексуальні вподобання, стає надбанням третіх осіб. Регламент (ЄС) 2016/679 гарантує користувачу конфіденційність. Обов'язки з захисту інформації регулюються статтями 6, 25, 28 та 32 [25; 26].

Експерти, політики і підприємці по-різному оцінюють запровадження нових норм. Як і будь-яке інше нововведення, нове положення про захист даних містить ще багато відкритих питань. На нашу думку, новиною Регламенту (ЄС) 2016/679 є введення таких понять, як "контролер", "оператор" та "співробітник захисту даних", які мають створити умови технічного та організаційного забезпечення, котре буде гарантувати відповідність вимогам з приводу дотримання прав суб'єкта даних.

На підставі викладеного ми дійшли висновку, що Регламент (ЄС) 2016/679 дозволить створити міцнішу законодавчу базу із захисту персональних даних для громадян ЄС і, як наслідок, такий захист буде мати вплив на світову систему захисту інформації.

Більшість держав відреагувала на підвищені останнім часом загрози національній безпеці шляхом розширення повноважень органів влади щодо доступу до особистої інформації, її збирання й опрацювання, які наразі не обмежені якимись окремими категоріями інформації. Все це загострює проблему забезпечення інформаційної безпеки людини і робить її виключно злободенною та актуальною. В контексті даного завдання посилюється необхідність найширшого залучення соціологічної науки, адже інформаційна агресія – це, перш за все, руйнування позитивних соціальних установок, базових цінностей, орієнтацій, відносин, зміна їх відповідно до інтересів, які властиві тим чи іншим антисоціальним елементам і силам. При цьому в різних державах підходи до забезпечення пропорційності вжитих заходів щодо забезпечення національної безпеки також можуть відрізнятися.

Міжнародна практика свідчить, що чим менше значення демократичних цінностей у політичному режимі, тим більшу роль відіграє забезпечення національної безпеки для збереження існуючого порядку управління державою, наслідком якого є встановлення різних обмежень прав людини, включаючи право на недоторканність приватного життя. Згідно з позицією Європейського суду з прав людини, вираженою в справі "Клас та інші проти Німеччини": …*"право таємного спостереження за громадянами, яке характерно для поліцейської держави, терпимо відповідно до Конвенції тільки тоді, коли воно суворо необхідно для збереження демократичних інститутів"*; держави *"не можуть в ім'я боротьби проти шпигунства і тероризму робити будь-які дії, які вони вважають потрібними"* [23].

На нашу думку, в структурі інформаційної безпеки слід інституціоналізувати систему засобів, методів та способів протидії. Вона має передбачати оптимальний (найбільш дієвий в сформованих умовах) підбір суб'єктів задля обмеження або блокування негативних інформаційних потоків і каналів. Суб'єкти мають володіти достатньою дієздатністю і правоздатністю у "відсіканні" деструктивної інформації. Важливо, щоб координація та взаємодія були налагодженими в часі та просторі, були оперативні і рухливі, володіли достатнім ступенем гнучкості. Система засобів, методів, способів протидії має враховувати особливості сприйняття інформації тими чи іншими соціальними групами населення, їх віковий, освітній, професійний, сімейний цензи, національність, загальний фон національної культури.

Необхідно, щоб система протидії керувалася рядом принципів, таких як:

1) соціальної значущості і доцільності, забезпечення інтересів більшості населення країни;

2) принцип найширшої гласності і демократії на основі об'єктивності і адекватності інформації сучасної дійсності;

3) принцип дотримання прав людини;

4) принцип гуманності;

5) принцип збереження соціальної стабільності;

6) принцип загальноприйнятої людської моралі і моральності;

7) принцип всебічного духовного, культурного і інтелектуального розвитку людини як головного творця історичного прогресу.

Серед конкретних напрямів реалізації принципів слід виділити: контрінформацію, деідеологізацію, правове, організаційне блокування негативної інформації, парламентський, громадський і громадянський контроль за інформацією, що надається людині на змістовному і інституціональному рівні.

Зазначимо, що в нашій країні питання забезпечення інформаційної та інформаційно-психологічної безпеки вже почало опрацьовуватись. Так, Українським центром економічних досліджень в 2011 році проведений системний аналіз ситуації у сфері інформаційної безпеки України. До основних загроз інформаційної безпеки України експерти віднесли: обмеження свободи слова та доступу громадян до інформації; руйнування системи цінностей, духовного та фізичного здоров'я особи, суспільства, негативні зміни їх цільових настанов; маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл; низький рівень інтегрованості України у світовій інформаційний простір тощо [27, с. 29]. Проте такі дослідження мають здійснюватися на регулярній основі.

Висновки.

Підсумовуючи зазначене, можна констатувати, що інформаційна безпека – це такий стан соціуму, в якому забезпечений надійний і всебічний захист людини,

суспільства та держави від впливу особливого виду загроз, які виступають в формі організованих або стихійно виникаючих інформаційних потоків, що здійснюються в інтересах регресивних, реакційних або екстремістські налаштованих політичних і соціальних сил і спрямованих на усвідомлену деформацію суспільної та індивідуальної свідомості, наслідком чого виступає девіантна поведінка особи, посилення соціально-політичних, економічних і духовних колізій, наростає психологічна напруженість соціуму тощо.

Якісне правове забезпечення інформаційної безпеки можливе тільки тоді, коли воно буде побудоване на сукупності наукових принципів, до яких можна віднести:

1. Законність і правова забезпеченість. Реалізуючи цей принцип, важливо домогтися невідворотної адміністративної та судової відповідальності за неправдиву інформацію.

2. Баланс інтересів особи, суспільства та держави. Даний принцип має бути спрямований на забезпечення оптимального співвідношення конфіденційної інформації та інформації, що викриває антисоціальні елементи суспільства.

3. Об'єктивність, науковість – з метою об'єктивного відображення існуючих реалій.

4. Інтеграція з міжнародними системами безпеки, чого нагально вимагають закономірності глобальної інтеграції та розвиток міжнародних комунікацій.

5. Економічна ефективність – результати від заходів інформаційної безпеки мають перевищувати сукупні витрати на них.

6. Комплексність, системність – тісний зв'язок всіх видів безпеки, засобів, методів і способів її забезпечення у часі та просторі.

Ключовими принципами формування державної політики у сфері забезпечення інформаційної безпеки людини мають стати:

- визнання особи як ключового і найбільш уразливого учасника інформаційних відносин;

- відповідальність держави в інформаційній сфері;

- відповідність вжиття організаційно-правових заходів безпеки реальним викликам і загрозам;

- недоторканність приватного життя (неприпустимість збору, зберігання, використання і поширення інформації про приватне життя особи без її згоди, обмеження доступу третіх осіб до інформації, контроль її цільового використання тощо);

- достовірність та цілісність інформації (особа, яка є суб'єктом права на інформацією або правом доступу до інформації, має право вимагати забезпечення її цілісності, тобто перебування в незмінному вигляді, забезпечення невтручання в структуру (форму) і зміст інформації;

- прозорість, відкритість та доступність інформації про діяльність суб'єктів владних повноважень (державних органів, органів місцевого самоврядування тощо). Можуть бути введені обмеження цього принципу, які мають відповідати за змістом та обсягом цілям обмежень і застосовуватися тільки для захисту інших рівнозначних правових цінностей;

- контроль за забезпеченням інформаційної безпеки людини. При цьому доцільно введення такого механізму, як моніторинг стану її захищеності від внутрішніх і зовнішніх загроз в інформаційній сфері.

Щодо захисту персональних даних людини, ми погоджуємось з думкою вчених щодо необхідності належного захисту даних, при якому необхідно дотримуватись таких принципів:

- персональні дані мають збиратися і оброблятися тільки відповідно до закону та тільки наділеними відповідними повноваженнями органами;

- персональні дані повинні бути адекватними відповідним зазначеним цілям, розпорядження ними має бути обмежено за термінами, бути точним і оброблятися тільки за згодою суб'єктів цих даних;

- персональні дані повинні бути доступні суб'єктам цих даних, у тому числі і для внесення уточнення в ці дані та ін.

У період посилення загроз національній безпеці зазвичай розширюються повноваження органів влади щодо доступу до особистої інформації, її збирання й опрацювання, які сьогодні не обмежені якимись окремими категоріями інформації, що у свій час загострює проблему забезпечення інформаційної безпеки людини. У цьому випадку, на наш погляд, юридична наука покликана виявити відхилення соціуму від позитивних соціальних установок, базових цінностей та орієнтацій відповідно до інтересів, які властиві тим чи іншим антисоціальним елементам чи силам, адже інформаційна агресія – це, перш за все, руйнування зазначених стереотипів.

В структурі інформаційної безпеки слід інституціоналізувати систему засобів, методів та способів протидії. Вона має передбачати оптимальний підбір суб'єктів задля обмеження або блокування негативних інформаційних потоків і каналів. Суб'єкти мають володіти достатньою дієздатністю і правоздатністю у "відсіканні" деструктивної інформації. Важливо, щоб координація та взаємодія були налагодженими в часі та просторі, були оперативні і рухливі, володіли достатнім ступенем гнучкості. Система засобів, методів, способів протидії має враховувати особливості сприйняття інформації тими чи іншими соціальними групами населення, їх віковий, освітній, професійний, сімейний цензи, національність, загальний фон національної культури.

Необхідно, щоб система протидії керувалася рядом принципів, таких як: соціальна значущість і доцільність; забезпечення інтересів більшості населення країни; гласність і демократія на основі об'єктивності і адекватності інформації сучасній дійсності; дотримання прав людини, гуманність; збереження соціальної стабільності; принцип загальноприйнятої людської моралі і моральності, всебічного духовного, культурного і інтелектуального розвитку людини як головного творця історичного прогресу.

Перспектива подальших досліджень. Останнім часом дедалі дослідників і практиків звертають увагу на необхідність активної розробки проблематики інформаційно-психологічної безпеки особи, суспільства та держави. Логіка суспільного розвитку висуває ці проблеми до числа першочергових. Розгляд проблеми з науково-юридичної точки зору представляється особливо важливим, оскільки в основі більшості сучасних ІКТ і систем лежать суспільні процеси, а об'єктом їх впливу виступає конкретна особа в реальних історичних умовах.

Використана література

1. Про національну безпеку: Закон України від 21.06.18 р. № 2469-19. URL: http://zakon2.rada.gov.ua/laws/show/2469-19

2. 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. *Офіційний вісник України*. 2014. № 37. Ст. 28.

3. Стратегія забезпечення кібернетичної безпеки України / Національний інститут стратегічних досліджень, 2013 р. URL: http://www.niss.gov.ua/public/File/2013 _nauk_an_rozrobku/kiberstrateg.pdf

4. Проект Концепції інформаційної безпеки України / Міністерство інформаційної політики України. URL: http://mip.gov.ua/documents/30.html

5. Про внесення змін до деяких законів України щодо захисту інформаційного телерадіопростору України: Закон України від 05.02.15 р. № 159-VIII. *Відомості Верховної Ради України*. 2015. № 18. Ст. 131.

6. Олійник О.В. Інформаційна безпека України: доктрина адміністративно-правового регулювання: автореф. дис. …док. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Інститут законодавства Верховної Ради України. Київ, 2013. – 34 с.

7. Линник Г.М. Адміністративно-правове регулювання інформаційної безпеки України: автореф. дис. … канд. юрид. наук: 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право / Національний університет біоресурсів і природокористування України. Київ, 2013. 27 с.

8. Ющук Е.Л. Интернет-разведка: руководство к действию. Москва-Санк-Петербург: Вершина, 2007. 249 с.

9. Толубко В.Б. Інформаційна боротьба (концептуальні, теоретичні, технологічні аспекти: монографія. Київ: НАОУ, 2003. 320 с.

10. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право*. 2015. № 2. С. 111-120.

11. Пилипчук В.Г., Брижко В.М. Інформаційна безпека та приватність у сфері захисту персональних даних. *Інформація і право*. 2016. № 4(19). С. 60-70.

12. Брижко В. Правовий захист та безпека персональних даних: соціальний і комерційний аспекти. *Інформація і право*. № 3(26)/2018. С. 16-37.

13. Брижко В.М., Швець М.Я. е-боротьба в інформаційних війнах та інформаційне право: монографія / за ред. члена-кореспондента АПрН України, д.е.н., професора М. Швеця. Київ: НДЦПІ АПрН України, 2007 р. 236 с.

14. В Грузии приняли закон о “прослушке”. URL: http://www.inter fax.ru/world/551861

15. Кому в Грузии достанутся ключи от “прослушки”? URL: https://digital.report/ komu-v-gruzii-dostanutsya-klyuchi-ot-proslushki

16. Shaw T.J. Information security and privacy: A practical guide for global executives, law technologists. Chicago: American Bar Association. 2011. P. 17. URL: http://faculty.cbpa.drake.edu/ dmr/0101/DMR010113B.pdf

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

18. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI. URL: http://zakon3.rada.gov.ua/laws/show/2939-17

19. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. URL: http://zakon0. rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80

20. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних: Конвенція Ради Європи від 28 січня 1981 р. № 108 / офіційний переклад. засвідчено МЗС України 01.07.02 р.: у кн. *Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних*: посіб. / В. Брижко, М. Швець та ін. Кн. 2. Київ: ТОВ “ПанТот”, 2006. 509 с. С. 66-72.

21. Про захист прав людини і основоположних свобод: Європейська Конвенція від 4 листопада 1950 року / офіційний переклад засвідчено МЗС України 27.01.06 р.: у кн. *Системна інформатизація правоохоронної діяльності: європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних*: посіб. / В. Брижко, М. Швець та ін. Кн. 2. Київ: ТОВ “ПанТот”, 2006. 509 с. С. 34-59.

22. Пресс-Релиз № 70/14 Суда Европейського Союза (Люксембург, 13 мая 2014 года): Решение по делу С-131/12 “Марио Костея Гонсалес против Google Spain SL, Google Inc. v

Agencia Española de Protección de Datos": (оператор Интернет-поиска несет ответственность за обработку личных данных, которые появляются на веб-страницах, опубликованных третьими лицами). URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/ 2014-05/cp 140070en.pdf

23. Klass and Othersvs Germany, § 56, Series A, № 28. URL: https://www.stewartroom.co.uk/wp-content/uploads/2014/07/Cases-ECHR-Klass.pdf

24. Брижко В. Сучасні основи захисту персональних даних в європейських правових актах. *Інформація і право*. № 3(18)/2016. С. 45-57.

25. Пилипчук В.Г., Брижко В.М., Баранов О.А., Мельник К.С. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія / за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ "Видавничий дім "АртЕк", 2017. 226 с.

26. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів / переклад з англ. В. Брижко, кор. І. Майстренко / за ред. В. Брижко, передмова В. Пилипчука. / НДІ інформатики і права Національної академії правових наук України. Київ: ТОВ "Видавничий дім "АртЕк", 2018. – 180 с.

27. Актуальні проблеми інформаційної безпеки України: аналітична доповідь. *Національна безпека і оборона*. 2001. № 1. С. 2-59.

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

Правова інформатика

УДК 002.6:004:340.1+316.329.8

БАРАНОВ О.А., *доктор юридичних наук, с.н.с.,*
керівник Центру теоретико-правових проблем інформаційної сфери
НДІІП НАПрН України

ІНТЕРНЕТ РЕЧЕЙ (IoT): РЕГУЛЮВАННЯ НАДАННЯ ПОСЛУГ РОБОТАМИ ЗІ ШТУЧНИМ ІНТЕЛЕКТОМ

Анотація. *У статті досліджуються теоретико-правові засади регулювання надання послуг і проведення робіт з використанням технологій Інтернету речей зі штучним інтелектом за участю і без безпосередньої участі людини. Як типовий приклад розглядається система замовлення і доставки товарів. Запропоновано нові категорії – "безпосередні, опосередковані та гібридні правовідносини" для проведення аналізу правових моделей систем замовлення і доставки товарів з технологіями Інтернету речей зі штучним інтелектом. Досліджено особливості правових моделей детермінованого і робастного соціального управління, що адекватно описують системи Інтернету речей зі штучним інтелектом. Показана функціональна аналогія "поведінки" систем з Інтернету речей зі штучним інтелектом та традиційного суб'єкта права при здійсненні певної діяльності. Обґрунтовано нову теоретичну конструкцію категорії "юридична фікція" на основі запропонованого терміну "юридична догма". Запропоновано і обґрунтовано зміст юридичної фікції: система Інтернету речей зі штучним інтелектом розглядається як суб'єкт права в якості "представника" в розумінні цивільних правовідносин.*

Ключові слова*: правове регулювання, технологія, Інтернет речей, штучний інтелект, фікція, догма, представництво.*

Summary. *The article examines the theoretical and legal framework for regulating the provision of services and works using the technologies of the Internet of Things with artificial intelligence with and without direct human participation. As a typical example, a goods ordering and delivery system is considered. New categories are proposed – "direct, mediated and hybrid legal relations" for analysing the legal models of goods ordering and delivery system with IoT with artificial intelligence. The features of the legal models of deterministic and robust social management adequately describing IoT systems with artificial intelligence are investigated. The functional analogy of the "behaviour" of systems of IoT with artificial intelligence and traditional subjects of law when performing certain types of activities is shown. A new theoretical construction of the category "legal fiction" is justified on the basis of the proposed term "legal dogma". The content of legal fiction has been proposed and justified: the system of Internet of Things with artificial intelligence is considered a subject of law, as a "representative" in the understanding of civil legal relations.*

Keywords*: legal regulation, technology, Internet of Things, artificial intelligence, fiction, dogma, representation.*

Аннотация. *В статье исследуются теоретико-правовые основы регулирования оказания услуг и проведения работ с использованием технологий Интернета вещей с искусственным интеллектом при участии и без непосредственного участия человека. В качестве типового примера рассматривается система заказа и доставки товаров. Предложены новые категории – "непосредственные, опосредованные и гибридные правоотношения" для проведения анализа правовых моделей систем заказа и доставки товаров с технологиями Интернета вещей с искусственным интеллектом. Исследованы особенности правовых моделей*

детерминированного и робастного социального управления, адекватно описывающих системы Интернета вещей с искусственным интеллектом. Показана функциональная аналогия "поведения" систем Интернета вещей с искусственным интеллектом и традиционных субъектов права при осуществлении определенной деятельности. Обоснована новая теоретическая конструкция категории "юридическая фикция" на основе предложенного термина "юридическая догма". Предложено и обосновано содержание юридической фикции: система Интернета вещей с искусственным интеллектом рассматривается как субъект права в качестве "представителя" в понимании гражданских правоотношений.

Ключевые слова: *правовое регулирование, технология, Интернет вещей, искусственный интеллект, фикция, догма, представительство.*

Постановка проблеми. Політичні і державні діячі, вчені та практики, економісти і соціологи, технічні фахівці і гуманітарії з наростаючою інтенсивністю ведуть дискусії на тему майбутнього цивілізаційного розвитку. Серед багатьох теорій і концепцій розвитку людства в останні 15 – 10 років особливу увагу привертає тема впровадження і використання технологій Інтернету речей (IP, Internet of Things, IoT) практично у всіх сегментах соціальної активності людства.

В літературі наводяться численні приклади надання послуг і проведення робіт з застосуванням технологій Інтернету речей як з участю людини, так і без її участі. Прикладом можуть слугувати: надання е послуг з дистанційного моніторингу інструментальних показників стану здоров'я людини [39; 41], проведення без участі людини різноманітних робіт у промисловій індустрії (роботизація) [37; 42], проведення профілактичних заходів при у процесі видобитку нафти [36], аграрні роботи в сільському господарстві [43], виконання різних робіт у сфері комунального господарства [44], послуги з роздрібного продажу товарів та їх доставка до споживача [19], транспортні послуги [45] і багато чого іншого.

Надання послуг і проведення робіт без участі людини стає можливим завдяки використанню штучного інтелекту (далі – ШІ), який фактично буде виконувати функції людини в процесі здійснення певної діяльності. Тому прогнозують, що досить поширеними стануть випадки, коли як з боку клієнта або замовника послуг і робіт, так і з боку виконавця будуть виступати роботизовані системи зі штучним інтелектом (роботи з ШІ) [6].

У цих умовах вивчення правової природи суспільних відносин, пов'язаних з наданням та проведенням послуг і робіт з використанням технологій Інтернету речей зі штучним інтелектом, є актуальним в контексті формування підходів до організації перспективних правових досліджень, ще до виникнення в практичній площині проблем, які будуть неодмінно з'являтися в результаті широкого застосування цих технологій.

Мета статті полягає в розвитку теоретико-правових засад регулювання надання послуг і проведення робіт з застосуванням технологій Інтернету речей зі штучним інтелектом за участю і без безпосередньої участі людини.

Виклад основного матеріалу. З метою використання в рамках даного дослідження, базуючись на результатах, отриманих в більш ранній роботі автора [5], наведемо деякі вихідні положення (при цьому необхідно звернути увагу на те, що згадувані раніше терміни "комплекси і системи IP з штучним інтелектом" еквівалентні термінам "робот-андроїд і простий робот"):

штучний інтелект (ШІ) *– це деяка сукупність методів, способів і засобів, зокрема, апаратних, та комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції (КФ) достатньою мірою еквівалентні когнітивним функціям людини;*

прикладний ШІ *(ПШІ, Applied Artificial Intelligence, AAI) – це ШІ, який максимально наближено імітує (моделює) одну або кілька когнітивних функцій людини та який використовується при реалізації конкретної діяльності без участі людини для досягнення поставлених цілей відповідно до заздалегідь визначених критеріїв і параметрів;*

загальний ШІ *(ЗШІ, Artificial General Intelligence, AGI) – це ШІ, який еквівалентно імітує (моделює) безліч когнітивних функцій людини та який застосовується при реалізації будь-якого виду діяльності без участі людини для досягнення поставлених цілей відповідно до визначених критеріїв та параметрів;*

простий робот *(simple robot) – інтеграція прикладного ШІ і технічної системи, що дозволяє реалізовувати одну або кілька когнітивних функцій людини в процесі здійснення конкретного виду діяльності, пов'язаної, як правило, з однорідними об'єктами, що мають матеріальний або нематеріальний зміст;*

робот-андроїд *(robot android) – інтеграція загального ШІ і технічної системи, що дозволяє реалізовувати безліч когнітивних функцій, в тому числі, праксис (цілеспрямовану рухову активність), в процесі здійснення будь-якого виду діяльності без участі людини, пов'язаної з різнорідними об'єктами, що мають матеріальний або нематеріальний зміст.*

Розглянемо правову модель надання послуг за допомогою технологій IP на прикладі найбільш масової в ритейлі системи дистанційного замовлення і доставки товарів. Спочатку розглянемо традиційний випадок – споживач і звичайний супермаркет (мегамаркет), іноді ще й кур'єр, який доставляє замовлення споживачу. Для цього традиційного випадку модель правовідносин виглядає наступним чином (Мал. 1), де:

Мал. 1. Традиційні правовідносини

1. *Суб'єкти правовідносин* – фізичні або юридичні особи, які безпосередньо укладають договір поставки товарів і беруть участь в його виконанні;

2. *Об'єкт правовідносин* – це складний об'єкт: набір товарів, наприклад, продуктів харчування, діяльність і поведінка суб'єктів з приводу формування та передачі замовлення на доставку конкретного переліку товарів, узгодження переліку товару для включення в замовлення, формування набору товарів відповідно до замовлення, доставка замовлення до споживача; прийом замовлення, оплата замовлення і доставки;

3. *Зміст основних правовідносин* – це зміст договору поставки товару, а також це правові норми національного законодавства, які в режимі загального регулювання мають відношення до такого роду договорів.

4. *Зміст інформаційних правовідносин* – це права, обов'язки і відповідальність суб'єктів (сторін договору) в процесі їх інформаційної взаємодії.

Контракт може передбачати різні варіанти поставки товарів споживачу:

– фіксований постійний набір товарів, які періодично поставляються в певний день тижня або на певну дату;

– варіативний набір товарів, перелік яких кожен раз спрямовується до супермаркету і остаточний варіант узгоджується зі споживачем із зазначенням дати поставки;

– змішаний варіант, що складається з перших двох, коли набір товарів складається з фіксованої частини товарів, що постійно поставляються, та варіативної частини, в якій перелік продуктів може змінюватися.

Безсумнівно, суспільні відносини, пов'язані з укладенням контракту і його виконанням, супроводжуються відповідними інформаційними правовідносинами між суб'єктами основних правовідносин. Ці інформаційні відносини можуть бути реалізовані у найрізноманітніший спосіб:

– на стадії укладення контракту – усний (в процесі проведення переговорів), письмовий (документи, поштові відправлення), по телефону, за допомогою мережі Інтернет (електронна пошта) тощо;

– на стадії виконання контракту – як правило, замовлення здійснюються по телефону, за допомогою мережі Інтернет (електронна пошта) тощо.

У деяких країнах подібні контракти з огляду на їх поширеність регулюються законодавством щодо публічного договору. У законодавстві України (Цивільний кодекс України, ст. 633) визначається, що публічним є договір, в якому одна сторона – підприємець бере на себе обов'язок здійснювати продаж товарів, виконання робіт або надання послуг кожному, хто до неї звернеться (роздрібна торгівля, перевезення транспортом загального користування, послуги зв'язку, медичне, готельне, банківське обслуговування тощо). При цьому умови публічного договору встановлюються однаковими для всіх споживачів, крім тих, кому за законом надані відповідні пільги, а підприємець не має права надавати перевагу одному споживачеві перед іншим при виконанні публічного договору, якщо інше не встановлено законом.

Але за наявності якихось особливостей або деякої ексклюзивності контракту продажу та постачання товарів, він може укладатись в письмовій формі з кожним споживачем окремо. В інтересах цього дослідження особливостей правового регулювання надання послуг в умовах використання технологій ІР з ШІ будемо розглядати другий варіант з укладанням письмового договору як найбільш поширений в разі тривалої та варіативної співпраці.

Найчастіше контракт спочатку укладається у формі рамкового на поставку товарів, а оформлення замовлень на поставку конкретного, зокрема, варіативного переліку товарів – у формі локальних контрактів, що укладаються в рамках загального контракту. Юридично локальні контракти на поставку конкретного (варіативного) набору товарів, які реалізуються на виконання рамкового контракту, є його невід'ємною частиною. Відповідно до положень рамкового контракту такі локальні контракти можуть документуватися, як може документуватися і сам факт виконання замовлення.

Таким чином, правовідносини, пов'язані із замовленням споживачем і постачанням супермаркетом йому відповідно до цього замовлення товарів при безпосередній взаємодії суб'єктів права, складаються з двох основних частин:

– перша частина – правовідносини безпосередньо між його суб'єктами, які пов'язані з укладанням ними рамкового контракту;

– друга частина – правовідносини безпосередньо між його суб'єктами, які пов'язані з укладанням та виконанням ними локальних контрактів поставки конкретного переліку товарів та їх доставки споживачу.

Описана правова модель надання послуг з доставки замовлених товарів є поширеною і, як правило, додаткових питань не викликає.

Проте, застосування технологій ІР з ШІ призводить до необхідності зміни правової моделі надання послуги замовлення та доставки товару. Наведемо для прикладу широко відомий домашній холодильник, який, функціонуючи з використанням технологій ІР з елементами ШІ, самостійно, без участі споживача (власника цього холодильника), замовляє доставку товарів з супермаркету. На роботизованому складі супермаркету формується набір продуктів відповідно до замовлення та доставляється споживачеві. Холодильник в такій конфігурації можна назвати робот-холодильник, а супермаркет – робот-склад.

Для описаного варіанту надання послуги послідовність дій щодо замовлення товарів, виконання і доставки замовлень можна представити таким чином.

1. Суб'єкти права (споживач і супермаркет) укладають рамковий контракт поставки товарів. Предметом цього договору є: поставка товарів (продукти харчування), процедури оформлення, формування, доставки замовлення, його прийом, ціна надання послуги тощо, а також зміст локальних контрактів.

2. Основною відмінністю такого контракту від звичайних є положення, що стосуються процедур замовлення товарів, формування замовлення і його доставки з використанням технологій ІР з ШІ: робота-холодильника та робота-складу.

3. Робот-холодильник формує список товарів, що мають бути замовлені та відсилає його роботу-складу.

4. Робот-склад формує замовлення і доставляє його замовнику, наприклад, за допомогою дронів.

6. Підтвердження роботом-холодильником факту отримання замовлення та здійснення розрахунку.

В умовах використання технологій ІР оформлення, формування, доставка замовлення та його прийом технологічно здійснюється досить легко:

– сенсори у роботі-холодильнику фіксують відсутність тих чи інших продуктів або критичне зменшення їх кількості;

– ШІ робота-холодильника, обробляючи цю інформацію, а також аналізуючи накопичену інформацію про смаки і звички споживача, про майбутні події в його житті (вихідні дні, поїздка на пікнік, свята тощо) формує список продуктів, що мають бути замовлені, який складається з двох частин: постійної і варіативної;

– повідомлення містить інформацію про список продуктів, що замовляються, робот-холодильник спрямовує за допомогою мережі передачі даних (мережі Інтернет) в супермаркет;

– робот-склад (супермаркет), який використовує технології ІР з ШІ, формує список продуктів для виконання замовлення;

– ШІ робота-складу, аналізуючи замовлення та наявний запас продуктів на складі, пропонує еквівалентну або близьку за певними характеристиками заміну відсутніх в даний момент часу замовлених продуктів;

– робот-склад у разі внесення змін до номенклатури продуктів що замовлялись, відсилає сформований список продуктів роботу-холодильника на узгодження;

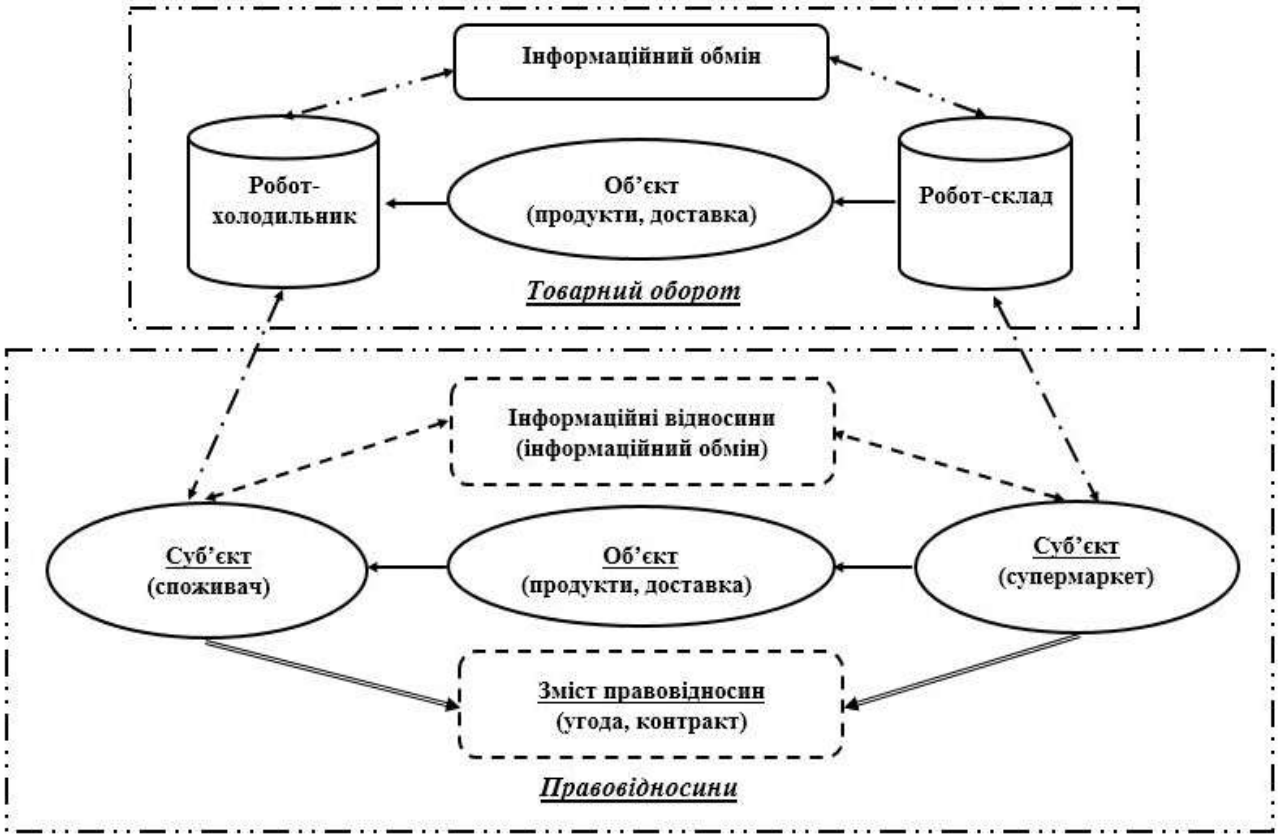
– ШІ робота-холодильника аналізує запропоновані зміни в номенклатурі продуктів, накопичені великі дані щодо свого власника, наявні інструкції за своїми

повноваженнями і діями, формує остаточно узгоджений список продуктів і відсилає його роботу-складу;

– робот-склад після отриманого погодження від робота-холодильника, з урахуванням висловлених побажань, за допомогою системи ІР формує контейнер із замовленими продуктами і за допомогою дронів спрямовує його споживачеві. При цьому ШІ робота-складу визначає маршрут руху дрона відповідно до адреси доставки, сповіщаючи робота-холодильник про доставку замовлення;

– робот-холодильник, отримавши інформацію про прибуття контейнера, зчитує з нього дані про фактичний склад надісланих продуктів і, в разі відсутності зауважень щодо їх складу і якості, здійснює оплату відповідно до рахунку робота-складу.

Модель правовідносин між споживачем і супермаркетом для випадку використання технологій ІР ілюструється на Мал. 2.



Мал. 2. Правовідносини в умовах застосування ІР

Інформаційні відносини в умовах використання технологій ІР дещо видозмінюються. На стадії укладення рамкового контракту вони залишаються незмінними, тобто інформаційні відносини здійснюються безпосередньо між суб'єктами правовідносин. А ось в частині виконання контракту, тобто в умовах виконання локальних контрактів, інформаційний обмін здійснюється між елементами систем ІР споживача (робот-холодильник) і супермаркету (робот-склад) шляхом формування та пересилання інформаційних повідомлень за допомогою мережі передачі даних (мережі Інтернет) без безпосередньої участі суб'єктів правовідносин.

Отже, при реалізації правовідносин, пов'язаних із замовленням товарів споживачем і постачанням йому цих товарів супермаркетом, частина дій може відбуватись за допомогою технологій ІР без безпосередньої взаємодії суб'єктів цих правовідносин. При цьому можливі два варіанти "поведінки" технологій ІР з ШІ.

Варіант 1. Замовлення виконується за строго заздалегідь заданим споживачем списком можливих продуктів без варіативної частини. Рішення приймає ШІ робота-холодильника, у якого реалізовані лише ті когнітивні функції, які необхідні для:

– збору інформації від датчиків;

– формування списку замовлення продуктів;

– передачі інформації з цього списку;

– прийому інформації про доставку замовлення та його вартість;

– розрахунки за доставлене замовлення за заздалегідь заданими реквізитами.

Робот-холодильник в цьому випадку при формуванні замовлення продуктів "поводиться" в суворій відповідності з жорстко детермінованою послідовністю дій. У разі відсутності будь-якого товару його заміна не проводиться.

Варіант 2. Замовлення здійснюється у відповідності до рамкових "вказівок" споживача щодо номенклатури, кількості та якості продуктів. Рішення приймає ШІ робота-холодильника, у якого в порівнянні з першим варіантом додані наступні когнітивні функції:

– аналізу, в тому числі, кореляційного та крос-факторного, різноманітної інформації;

– синтезу інформації для прийняття рішення;

– формування мети, яка може бути варіативною в залежності від отриманої інформації;

– самонавчання на основі отриманої інформації та досвіду;

– самостійного прийняття рішення.

Робот-холодильник в цьому випадку при формуванні замовлення продуктів "поводиться" відповідно до прийнятих ним рішенньі (з його "волі"), зміст яких залежить від параметрів зовнішніх або внутрішніх умов виконання ним функції щодо своєчасного забезпечення споживача продуктами із заздалегідь визначеними вимогами щодо їх номенклатури, кількості та якості.

У відповідності з наведеними вище в статті визначеннями, для варіанта 1: робот-холодильник можна вважати простим роботом, а для варіанта 2: робот-холодильник – робот-андроїд.

Необхідно мати на увазі, що всі дії, які здійснюються у відповідності з прийнятими простим роботом або роботом-андроїдом "рішеннями", мають юридичні наслідки для реальних суб'єктів правовідносин, незважаючи на те, що вони безпосередньої участі в них не беруть.

Виходячи з класичного визначення правовідносини, можливо стверджувати, що це завжди вольові суспільні відносини безпосередньо між суб'єктами, які регулюються нормами права в частині встановлення суб'єктивних прав, обов'язків і відповідальності цих суб'єктів по відношенню один до одного [7; 20; 32]. Підкреслюючи безпосередність відносин між суб'єктами правовідносин, ми тим самим звертаємо увагу на наявність безпосередньої інформаційної взаємодії між ними. Наявність безпосередньої інформаційної взаємодії між суб'єктами права і безпосереднього виявлення ними волі на вчинення тієї чи іншої дії (бездіяльності) є визначальним на всіх етапах правовідносин: формування, фіксації та реалізації.

Теорія права допускає випадки, коли правовідносини здійснюються не безпосередньо суб'єктом цих відносин, а його представником, який наділяється відповідними повноваженнями. Але, в цих випадках, представник суб'єкта права може діяти лише строго в рамках повноважень, які надані йому або законом, або суб'єктом, і виключно в інтересах суб'єкта, якого він представляє. В українському законодавстві

таке положення закріплено в Цивільному кодексі в статті 237: “представництвом є правовідношення, в якому одна сторона (представник) зобов’язана або має право вчинити правочин від імені другої сторони, яку вона представляє”. Досить розгорнуте розуміння інституту представництва, як правового явища, надано Е.О. Харитоновим, за думкою якого [34] :

– представництво є юридичним прийомом, який забезпечує більш повну можливість реалізації прав і здійснення обов’язків учасниками приватного (цивільного, економічного, торгового) обігу;

– діяльність представника за своїм характером є правомірною діяльністю; представництво є системою правовідносин, в рамках яких одна особа (представник) юридично допомагає іншій особі в придбанні і реалізації суб'єктивних прав і обов'язків останнього в його відносинах з третіми особами;

– представництво можливо тільки щодо суб’єкта права; діяльність представника повинна здійснюватися в інтересах представленого;

– можливість, зміст і межі зазначеної допомоги визначаються повноваженнями представника;

– в процесі здійснення повноваження представник діє щодо третіх осіб, з якими у нього не виникає прав і обов’язків.

Звернемо увагу на те, що інформаційна взаємодія в рамках основних правовідносин здійснюється безпосередньо між представником суб’єкта й іншим суб’єктом. Інформаційна взаємодія між представником суб’єкта і суб’єктом, чиї інтереси він представляє, здійснюється в рамках інших правовідносин, об’єктом якого є власне представництво. Цілком є припустимою ситуація, коли з боку всіх суб’єктів права можуть виступати представники, що досить часто спостерігається на практиці.

Представник, діючи від імені суб’єкта, приймає вольові рішення з всього спектру питань, пов’язаних з даними правовідносинами, в межах повноважень наданих йому суб’єктом, результат реалізації яких повинен завжди відповідати інтересам цього суб’єкта.

Поділяючи погляди Е.О. Харитонова на зміст інституту представництва, в цілях подальших досліджень дамо наступні визначення:

безпосередні правовідносини *– це правовідносини, які реалізуються безпосередньо його суб’єктами при наявності інформаційної взаємодії між ними;*

опосередковані правовідносини *– це правовідносини, які реалізуються опосередковано представниками на основі делегування їм суб’єктами цих правовідносин вичерпно певної частини своїх прав і обов’язків при наявності інформаційної взаємодії як між представниками, так і між суб’єктами. Отже, опосередковані правовідносини – це такі правовідносини, в яких хоча б один суб’єкт бере участь через представника;*

гібридні правовідносини *– це комплексні, складні правовідносини, в яких їх суб’єкти беруть безпосередню участь в одній частині суспільних відносин, а інша частина суспільних відносин між суб’єктами здійснюється без їх участі за допомогою посередників. Гібридні правовідносини згідно з їх юридичною природою – це завжди сукупність безпосередніх і опосередкованих правовідносин.*

Таким чином, можна констатувати, що правовідносини, пов’язані із замовленням споживачем і постачанням супермаркетом відповідно до цього замовлення продуктів з застосуванням технологій ІР з ШІ, складаються з двох частин (Мал. 2 і 3):

а) формування правовідносин – *безпосередні правовідносини*: укладення рамкового контракту безпосередньо між суб’єктами правовідносин;

б) реалізація правовідносин – *опосередковані правовідносини*: “укладання” та виконання локальних контрактів поставки переліку продуктів здійснюється за допомогою робота-холодильника, який фактично виступає “представником” споживача, і – робота-складу, який є “представником” супермаркету.

У реальному житті, звичайно, досягнення більшості соціальних цілей відбувається за допомогою реалізації комплексних, складних правовідносин, які являють собою сукупність різноманітних простих правовідносин. Це відноситься і до правовідносин між споживачем і супермаркетом. Так ось частина з цих правовідносин, яка здійснюється “представниками” від імені споживача та від імені супермаркету як суб’єктів, яких вони “представляють”, за формальними ознаками можна віднести до опосередкованих правовідносин. Однак, зазначені “правовідносини” мають одну істотну особливість, яка полягає в тому, що в якості “представників” суб’єктів права виступають не юридичні або фізичні особи, а технології ІР.

Заміна людини в деяких видах діяльності, яка має юридичні наслідки, спеціальними технічними і технологічними системами, наприклад, технологіями ІР, має не дуже давню історію. Тому вирішення правових проблем, що пов’язані з цим, поки ще не знайдено, але наукові дискусії з цього приводу інтенсивно розгортаються.

Ще раз звернемо увагу на те, що для випадків, подібних до описаного нами вище, найбільш раціональним є укладення (рамкової) угоди на надання якогось певного роду послуг, яка визначає правову основу для укладення подальшої серії індивідуальних контрактів “програмними агентами”, де в якості “програмних агентів”, наприклад, виступають комп’ютерні програми, що автоматично генерують запит на інформаційну послугу і автоматично надають запитувану інформаційну послугу [38]. При цьому стверджується, що програмні агенти можуть вести “переговори” тільки про зміст наданої послуги, але не про правові зобов’язання, що випливають зі змісту послуги, що надається.

Здавалося би, такий підхід відкриває шлях до можливості укладення так званих напівавтоматичних контрактів [3]. Однак, той факт, що у випадку гібридних правовідносин частина суспільних відносин реалізується без участі людей викликає питання, наприклад, такі: як регулювати взаємодію систем ІР, якщо його результати є юридично значущими для суб’єктів права; яким чином визначати права і обов’язки, відповідальність суб’єктів таких гібридних правовідносин; чи можна визнавати прийняті системами ІР “рішення” юридично значущими?

Спроби “втиснути” гібридні правовідносини безпосередньо в сучасну систему права видаються досить фантастичними через наявність практично непереборних бар’єрів концептуального характеру. Сучасна правова система багатьох держав доктринально передбачає правове регулювання суспільних відносин тільки між суб’єктами права, тобто тільки між фізичними або юридичними особами, або іншими суб’єктами, передбаченими законодавством. Такий класичний підхід принципово не передбачає розгляду систем ІР з ШІ в якості суб’єктів правовідносин. Однак, реальне життя, що очікує вибухове розширення масштабів використання технологій ІР, вимагає шукати рішення, максимально враховуючи реалії правових систем, які складалися протягом століть.

Отже, сформулюємо правову проблему, що стоїть перед юридичною наукою. Проблема – визначення засад правового регулювання суспільних відносин, які повністю або частково здійснюються на основі застосування систем ІР з ШІ.

Розглянемо взаємодію суб’єкта права та системи ІР з ШІ, що застосовується цим суб’єктом та яка призначена для виконання деяких дій (функцій) цього суб’єкта. При цьому реалізація цих функцій передбачає наявність суспільних відносин з іншим суб’єктом.

У загальному випадку модель процесу надання супермаркетом послуги замовлення та доставки товарів споживачам описується переліком таких дій (функцій):

1. Укладання рамкового контракту з супермаркетом на обслуговування (поставку товарів).

2. Укладання та виконання локальних контрактів:

2.1. Формування конкретного списку продуктів, що замовляються, і його передача супермаркету.

2.2. Реакція супермаркету про можливість виконання замовлення відповідно до поданого списку продуктів.

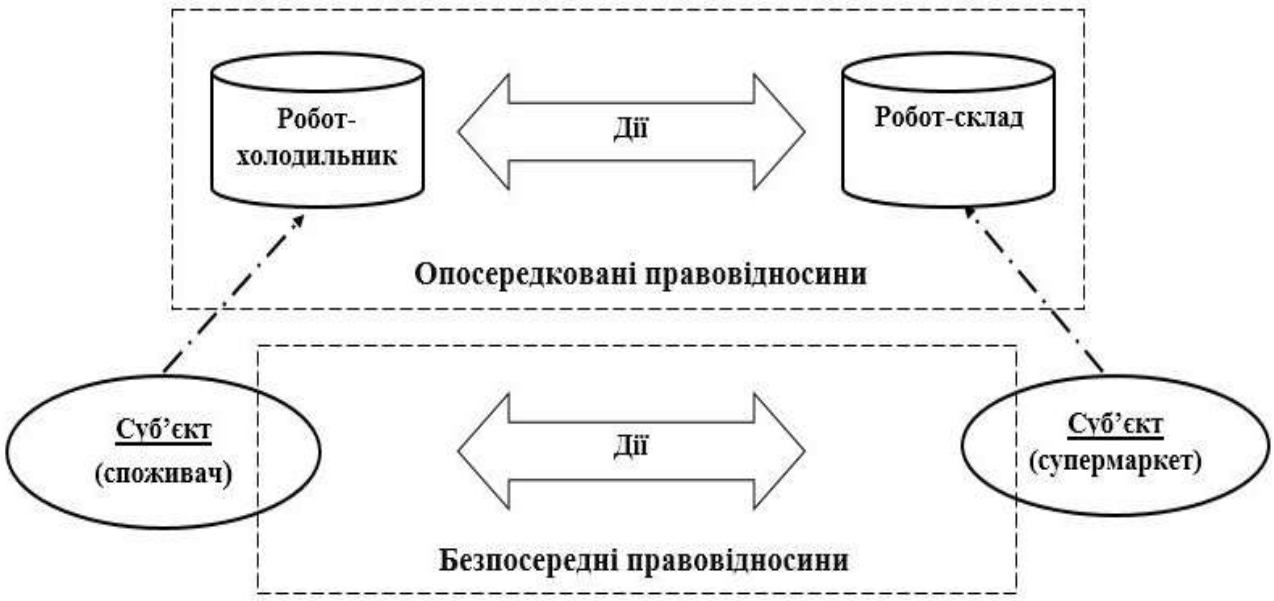
2.3. Можлива корекція замовлення.

2.4. Формування і доставка замовлення.

2.5. Підтвердження факту виконання замовлення.

2.6. Оплата виконаного замовлення.

На Мал. 3 схематично відображено ситуацію, коли функцію 1 реалізують безпосередньо суб'єкти правовідносин (супермаркет і споживач), а функція 2 реалізується за допомогою технологій ІР – це робот-холодильник і робот-склад.



Мал. 3

Відобразимо юридичну ситуацію, яка б відповідала моделі надання послуги (Мал. 3).

Якщо ми абстрагуємося від сутності систем ІР, та, використовуючи кібернетичний підхід, зосередимося тільки на їх функціях як "учасників" суспільних відносин, то приходимо до дійдемо висновку про те, що функції систем ІР з ШІ еквівалентні функціям представника суб'єкта права. Дійсно, з одного боку від "імені та за дорученням" суб'єкта (споживача) відповідно до заданого алгоритму і в межах встановлених обмежень робот-холодильник вчиняє дії з укладення та виконання локальних контрактів поставки продуктів з супермаркету (п. п. 2.1, 2.3, 2.5, 2.6), а з іншого боку від "імені та за дорученням" суб'єкта (супермаркету) відповідно до заданого алгоритму і в межах встановлених обмежень робот-склад вчиняє дії – п. п. 2.2, 2.4. Особливо підкреслимо, що це відбувається без безпосередньої участі суб'єктів цих правовідносин, але в їх інтересах.

Аналіз змісту безпосередніх і опосередкованих правовідносин (Мал. 2 і 3), дозволяє зробити висновок про те, що юридичні наслідки дій робота-холодильника і робота-складу є такими самими, як і юридичні наслідки дій традиційного (в юридичному сенсі) представника, уповноваженого на них суб'єктом.

У главі 17 Цивільного кодексу України (ЦКУ) встановлюється (статті 237-239), що:

– представництвом є правовідношення, в якому одна сторона (представник) зобов'язана або має право вчинити правочин від імені другої сторони, яку вона представляє;

– представництво виникає на підставі договору, закону, акта органу юридичної особи та з інших підстав, встановлених актами цивільного законодавства;

– представник може бути уповноважений на вчинення лише тих правочинів, право на вчинення яких має особа, яку він представляє;

– представник не може вчиняти правочин, який відповідно до його змісту може бути вчинений лише особисто тією особою, яку він представляє;

– правочин, вчинений представником, створює, змінює, припиняє цивільні права та обов'язки особи, яку він представляє.

При цьому беремо до уваги положення частини 2 статті 205 ЦКУ про те, що правочин, для якого законом не встановлена обов'язкова письмова форма, вважається вчиненим, якщо поведінка сторін засвідчує їхню волю до настання відповідних правових наслідків. Крім того, враховуємо положення частин 1 і 3 статті 206 ЦКУ про те, що усно можуть вчинятися правочини, які повністю виконуються сторонами у момент їх вчинення, за винятком правочинів, які підлягають нотаріальному посвідченню та (або) державній реєстрації, а також правочинів, для яких недодержання письмової форми має наслідком їх недійсність, і про те, що правочини на виконання договору, укладеного в письмовій формі, можуть за домовленістю сторін вчинятися усно, якщо це не суперечить договору або закону.

Отже, на підставі правових норм ЦКУ, детального функціонального і правового аналізу суспільних відносин, які складаються між споживачем і супермаркетом в процесі замовлення продуктів та їх доставки, в умовах застосування технологій ІР ми можемо сформувати наступну систему можливих юридичних аналогій для опосередкованих правовідносин (Мал. 2):

– представник – робот-холодильник, робот-склад;

– особа, яку представляє представник – споживач, супермаркет;

– представництво може виникнути на підставі договору, закону, акта органу юридичної особи та з інших підстав, встановлених актами цивільного законодавства;

– локальні контракти на виконання рамкового контракту між суб'єктами – споживачем і супермаркетом, укладеного в письмовій формі, можуть за домовленістю сторін вчинятися усно, якщо це не суперечить договору або закону;

– локальні контракти можуть вважатися усними, оскільки вони повністю виконуються сторонами в момент їх вчинення;

– локальні контракти, для яких законом не встановлена обов'язкова письмова форма, можуть вважатись виконаними, якщо дії (поведінка) представників свідчить про "волю" до настання відповідних наслідків.

Наведена юридична аналогія могла б привести до вирішення правової проблеми визначення основ правового регулювання суспільних відносин, які повністю або частково здійснюються на основі використання систем ІР, або, іншими словами, визначення правових механізмом регулювання суспільних відносин між споживачем і супермаркетом, пов'язаних з процесом замовлення продуктів та їх доставки в умовах

використання систем ІР з ШІ, якби не наступні обставини, пов'язані з представниками (робот-холодильник, робот-склад):

– як технічні системи, навіть реалізовані з використанням ШІ, вони не можуть бути стороною правовідносин і відповідно контракту (угоди);

– до них не може бути застосований термін "поведінка" в контексті ЦКУ.

Таким чином, приходимо до попереднього висновку про те, що в рамках традиційної системи права робот-холодильник, робот-склад, навіть незважаючи на те, що вони мають функціональну можливість замінити людину в рамках певної діяльності, не можуть бути визнані суб'єктами права.

В результаті аналізу сутності суспільних відносин приходимо до висновку про те, що суб'єктом права може бути особа, яка в сукупності має п'ять характеристик [4]:

1) є відокремленою однією зі сторін суспільних відносин;

2) може мати потенційну можливість брати участь в суспільних відносинах;

3) має реальну здатність брати участь в суспільних відносинах;

4) здатне брати участь в суспільних відносинах шляхом реалізації персональної волі, самостійно сформованої і вираженої;

5) при здійсненні вольової участі в суспільних відносинах набуває, реалізує і виконує персоніфіковані юридичні права і обов'язки.

Для теми нашого дослідження особливий інтерес представляє така характеристика суб'єкта як здатність брати участь в суспільних відносинах *шляхом реалізації персональної волі, самостійно сформованої і вираженої.*

Можливість самостійно формувати і висловлювати персональну волю визначається рівнем розвитку розумових здібностей (когнітивних функцій) людини. При цьому оцінка когнітивних функцій людини це фактично визначення наявності когнітивних порушень, їх тяжкості, якісних характеристик, гостроти розвитку, динаміки їх частоти і впливу на здатність суб'єкта до довільної регуляції своєї поведінки [8].

Отже, суспільні відносини – це безперервний ланцюжок самостійного формування і вираження власної волі суб'єктом з метою управління (регулювання) своєю поведінкою як результат реалізації деякої сукупності когнітивних функцій. Безсумнівно, на формування і вираження власної волі суб'єкта, як учасника правовідносин, фундаментальний вплив здійснюють системи права і законодавства. Отже, ми альтернативним шляхом приходимо до вже відомого висновку про те, що правове регулювання – це один з видів соціального управління. Відтак, система права – це система управління соціальною діяльністю (поведінкою суб'єктів) для досягнення заданих цілей.

Процес соціального управління або управління соціальною діяльністю для досягнення заданих цілей – це безперервний процес прийняття рішень [27]. Ми добре розуміємо, що управлінське рішення спрямоване на усунення протиріччя (ліквідацію відхилення), що виникає між початковим станом (фактичним станом) і метою діяльності (очікуваним станом) [21]. У свою чергу, рішення приймається на основі результатів аналізу інформації про розбіжності вихідного (поточного) і очікуваного стану, про параметри стану суб'єктів, що мають відношення до конкретної соціальної діяльності, про параметри стану внутрішніх і зовнішніх факторів, що впливають на соціальну діяльність тощо.

Таким чином, приходимо до наступного висновку: ***соціальне управління*** *– це безперервний ланцюжок взаємообумовлених рішень, які приймає суб'єкт в процесі реалізації суспільних відносин для досягнення мети соціальної діяльності шляхом управління своєю поведінкою і поведінкою інших суб'єктів за допомогою самостійного формування і вираження власної волі.*

В узагальненому вигляді будь-яка система управління соціальною діяльністю може бути описана наступним чином:

– суб'єкти: опис параметрів стану суб'єктів, які здійснюють діяльність, і суб'єктів, що впливають на прийняття ними рішень при здійсненні цієї діяльності;

– початковий стан: опис параметрів соціального середовища перед початком процесу соціального управління; опис параметрів початкових (вихідних) умов діяльності: юридичний статус суб'єктів, стан ресурсів (фінансових, організаційних, технічних, людських тощо), обмежень при здійсненні діяльності тощо;

– умови діяльності: опис параметрів стану середовища здійснення діяльності (внутрішніх і зовнішніх факторів, що впливають на її здійснення); опис діапазону допустимих змін параметрів стану суб'єктів, які здійснюють діяльність, і суб'єктів, що впливають на реалізацію діяльності; опис діапазону можливих змін параметрів стану середовища здійснення діяльності;

– мета діяльності: опис майбутнього (бажаного) значення параметрів стану соціального середовища як результату діяльності суб'єктів, а також можливо опис поточних допустимих значень параметрів стану соціального середовища.

Слід зазначити, що параметри станів, що описують систему управління соціальною діяльністю можливо умовно розділити на дві групи:

– стабільні значення параметрів: серед них, перш за все, – це параметри початкового стану і параметри мети діяльності, а також ті параметри, які не змінюють свого значення протягом усього процесу управління, наприклад, правила здійснення діяльності (законодавство);

– варіативні значення параметрів – параметри стану суб'єктів і параметри стану середовища здійснення діяльності, які детерміновано або випадковим чином можуть змінюватися в процесі соціального управління.

Відповідно до положень загальної теорії складних систем управління, виокремимо два можливих алгоритми управління (поведінки) соціальною діяльністю.

Детермінований алгоритм управління соціальною діяльністю *– це алгоритм управління, відповідно до якого рішення формується суб'єктом на початку процесу управління і залишається незмінним до його закінчення, а зміст рішення визначається значеннями параметрів змінних: початкового стану суб'єктів, середовища здійснення діяльності; мети діяльності.*

Для *детермінованого алгоритму управління соціальною діяльністю* характерним є те, що суб'єкт лише на початку приймає одне єдине рішення в частині управління своєю поведінкою і поведінкою інших суб'єктів за допомогою самостійного формування і вираження власної волі, що дозволяє йому з тим чи іншим рівнем ефективності досягти заданої мети. Алгоритм дій суб'єкта при цьому є незмінним. Ефективність використання такого алгоритму, як правило, висока тільки в умовах сталості значень параметрів змінних: початкового стану; мети діяльності; стану суб'єктів, стану середовища здійснення діяльності.

Адаптивний алгоритм управління соціальною діяльністю *– це алгоритм, відповідно до якого рішення формуються суб'єктом на початку процесу управління, а зміст першого рішення визначається значеннями параметрів: цілі діяльності; початкового стану суб'єктів, середовища здійснення діяльності, наступні зміни змісту рішення є реакцією на зміни параметрів стану суб'єктів і стану середовища здійснення діяльності, а іноді і мети здійснення діяльності.*

Для *адаптивного алгоритму управління соціальною діяльністю* характерним є те, що суб'єкт після прийняття першого рішення, реагуючи на зміни параметрів стану

суб'єктів і стану середовища здійснення діяльності, змушений щоразу змінювати (коректувати) свої рішення для того, щоб досягти заданої мети діяльності. При цьому, в силу ряду обставин, суб'єкт, як правило, не має можливості вимірювати або навіть виявляти всі зміни параметрів.

Алгоритм дій суб'єкта при цьому є варіативним, тобто він може змінюватися на різних етапах управління в залежності від значень параметрів стану суб'єктів і стану середовища здійснення діяльності, значення майбутніх змін яких в соціальному середовищі, як правило, слабо прогнозовані.

Тому для конкретної соціальної системи при заданих параметрах початкового стану і мети може формуватися безліч можливих варіантів управління соціальною діяльністю (поведінкою) в силу таких чинників:

– наявність помилок, неминучість яких обумовлена суб'єктивним характером процесу прийняття рішень як результату прояву волі суб'єкта і наявності помилок при вимірі параметрів стану суб'єктів і стану внутрішнього і зовнішнього середовища;

– наявність безлічі можливих поєднань варіативних значень параметрів стану суб'єктів та стану внутрішнього і зовнішнього середовища здійснення соціальної діяльності (поведінки). Власне, кожне з цих поєднань відповідає якомусь конкретному випадку реалізації адаптивного управління соціальною діяльністю.

Адаптивний алгоритм управління є найбільш ефективним в умовах стохастичних (випадкових) змін параметрів стану суб'єктів, середовища здійснення соціальної діяльності.

Таким чином, і детерміноване, і адаптивне управління (поведінка) при заданих параметрах початкового стану в певних умовах дозволяють досягти заданої мети соціальної діяльності. При цьому ми розуміємо, що система права має важливий вплив на вибір того чи іншого алгоритму поведінки суб'єкта в процесі здійснення соціальної діяльності.

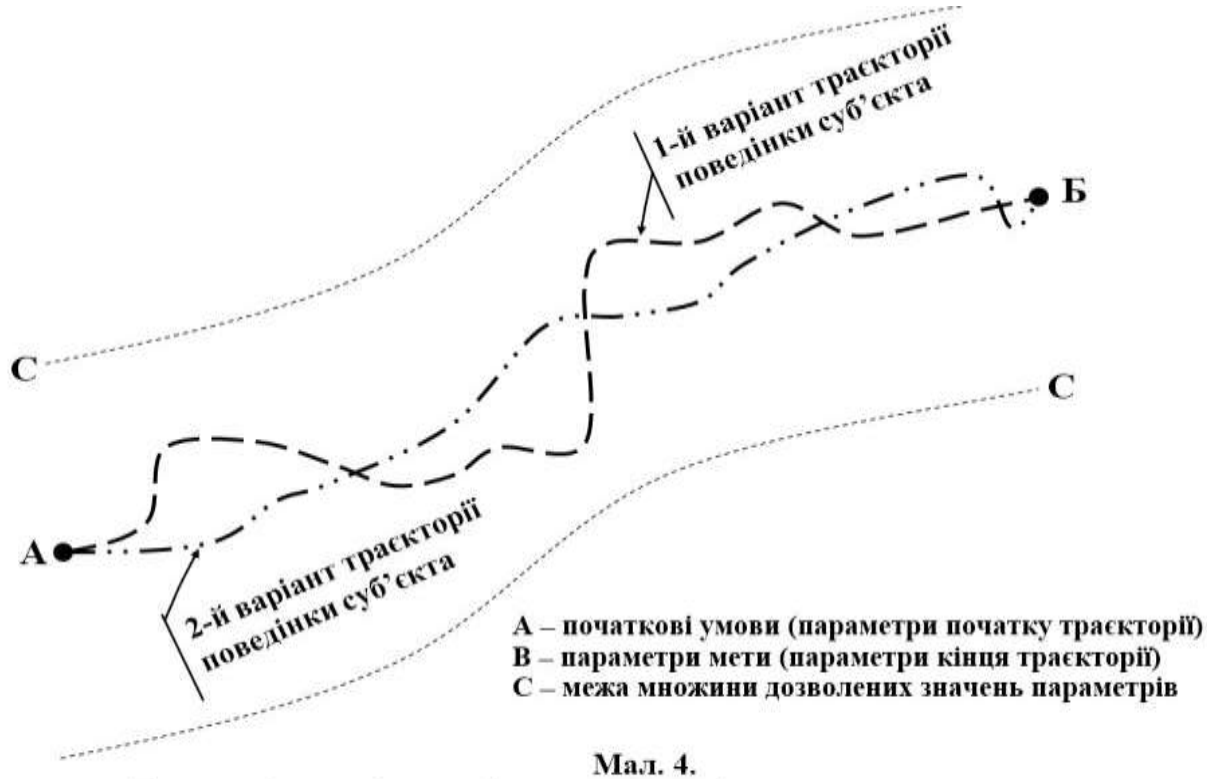
Спираючись на результати роботи Н. Вінера про єдність природи процесів управління (поведінки) в техніці, живій природі і суспільстві [10], висловимо припущення про те, що якась із ефективних моделей загальної теорії складних систем управління, яка описує функціонування технічних систем, зокрема, систем ІР з ШІ, може бути поширена і на випадок соціального управління.

В останні 40 – 50 років в рамках адаптивних алгоритмів управління активно розвивається теорія робастних систем управління. Робастність – властивість системи зберігати якість функціонування в межах вимог, що пред'являються до неї, шляхом змін її параметрів та/або структури [33]. Отримані і апробовані положення теорії робастного управління, які показали хороші результати в технічній галузі, в останні роки досить успішно застосовуються і в сфері соціального управління.

Використовуючи результати праць В. Афанасьєва [2] і Л. Варшавського [9], дамо наступне визначення терміну, максимального адаптованого для сфери правового регулювання: ***робастне соціальне управління*** *– соціальне управління, при якому однозначно задаються тільки початкові умови і мета діяльності (поведінки) суб'єкта, а параметри як всієї траєкторії його діяльності, так і будь-яких її ділянок визначаються волею суб'єкта в залежності від змін параметрів стану суб'єкта, зовнішніх та внутрішніх умов діяльності (правил, ресурсів тощо), які мають обмеження дозволених значень.*

Схематична ілюстрація моделі "робастне соціальне управління" наведена на Мал. 4, де: А - початкові умови (параметри початку траєкторії діяльності (поведінки) в системі координат параметрів стану); Б - параметри мети (параметри кінця траєкторії

діяльності); С - межа множини дозволених значень параметрів стану суб'єкта, зовнішніх і внутрішніх умов діяльності.



Мал. 4.
Траєкторії поведінки суб'єкта у просторі множини дозволених значень параметрів зовнішніх и внутрішніх умов и параметрів діяльності суб'єкта.

Другою моделлю соціального управління є ***детерміноване соціальне управління*** – *соціальне управління, при якому однозначно задаються параметри як початкових умов і мети діяльності (поведінки) суб'єкта, так і параметри всієї траєкторії його діяльності, які з одного боку визначаються його волею, але з іншого боку детермінуються волею іншого суб'єкта.* Яскравим прикладом соціального детермінованого управління є діяльність відповідно до вимог детальної інструкції з виконання якихось дій для досягнення суб'єктом поставлених цілей.

Суб'єкт права (юридична і фізична особа) в своїй практичній діяльності реалізує обидві ці моделі соціального управління:

– при виконанні певних інструкцій, положень, директивних норм права – детерміноване соціальне управління (поведінку);

– при досягненні заданої мети в умовах невизначеності параметрів стану зовнішніх і внутрішніх умов та нечіткої множини параметрів його діяльності, диспозитивних норм права – робастне соціальне управління (поведінку) .

Робастне соціальне управління є переважним видом поведінки суб'єкта права в умовах пізнання навколишнього світу, який постійно змінюється, та безперервності власної еволюції, що дозволяє з певним рівнем ефективності адаптуватися до поточних і майбутніх змін.

Аналіз показує, що для різної "поведінки" технологій ІР, що функціонально замінюють людину в певній діяльності, також будуть використовуватися різні види моделей соціального управління і, відповідно, різні види ШІ і роботів, які надають змогу їх реалізовувати.

Варіант 1. Замовлення здійснюється суворо за заздалегідь заданим споживачем переліком можливих продуктів без всіляких варіацій. Рішення приймає ШІ робота-холодильника у відповідності до жорстко детермінованої послідовності дій, у якого реалізовано обмежену кількість простих когнітивних функцій, необхідних для збору інформації, формування списку замовлення, передачі і прийому інформації, оплати.

У цьому випадку доцільно використовувати:

– модель детермінованого соціального управління (заданої "поведінки");
– ШІ – прикладний ШІ (Applied Artificial Intelligence, AAI);
– робот – простий робот (simple robot).

Варіант 2. Замовлення здійснюється у відповідності до рамкових "вказівок" споживача щодо номенклатури, кількості та якості продуктів. Рішення приймає ШІ робота-холодильника, який має додаткові когнітивні функції, необхідні для аналізу і синтезу інформації, формування мети, самонавчання, самостійного прийняття рішення. ШІ при цьому "поводиться" відповідно до прийнятих ним рішень (за його "волею"), зміст яких залежить від зміни параметрів стану зовнішніх або внутрішніх умов.

Для цього випадку потрібно використовувати:

– метод робастного соціального управління (гнучкої "поведінки");
– ШІ – загальний ШІ (Artificial General Intelligence, AGI);
– робот – робот-андроїд (robot android).

Таким чином, ми маємо протиріччя: з одного боку, доведена функціональна аналогія поведінки "представника" (робот-холодильник і робот-склад) та суб'єкта (споживач і супермаркет) при здійсненні певної діяльності, а з іншого боку, у юридичному сенсі такої аналогії їх діяльності принципово не може бути, оскільки це суперечить базовим положення системи права в частині визначення суб'єкта права.

Виявлене протиріччя призводить до правової невизначеності в частині регулювання суспільних відносин, пов'язаних з наданням послуг або проведенням робіт на основі застосування технологій ІР з ШІ з частковою участю або зовсім без участі людини.

Виявлена правова невизначеність є причиною появи низки бар'єрів на шляху розвитку ІР як перспективного виду технологій, тому необхідно провести дослідження з пошуку можливих шляхів її подолання.

Звернемо увагу на таку категорію як "юридична фікція", яка, на думку багатьох вчених, в правовій науці, в правотворчості і в правозастосуванні дозволяє подолати негативні наслідки правової невизначеності та одночасно надає можливості щодо використання вже напрацьованого правового теоретичного і практичного досвіду.

Дискусії навколо категорії "правова фікція" або "юридична фікція" ведуться досить давно, але широта використання цього юридичного феномена дозволяє припустити його практичну корисність для системи права.

Правова фікція (лат. fictio – "вигадка") – в найзагальнішому сенсі визначається як прийом, що полягає в тому, що дійсність підводиться під умовну формулу, яка не має реального змісту [24]. Давидова М.Л. вважає, що "... фікція має на увазі юридичне твердження, яке не допускає виключень з обов'язку визнати факти встановленими" [12]. На думку Е. Моглен, "юридичною фікцією є твердження в сфері матеріального або процесуального права, що претендує бути принципом або нормою для певних випадків, яке спирається, в цілому або в деталях, на фактичні передумови, про які заздалегідь відомо, що вони не відповідають дійсності" [40].

Частина авторів відводить юридичній фікції роль певного прийому юридичної техніки, наприклад, за допомогою якого конструюється юридично незаперечне але

помилкове положення, яким існуюче визнається неіснуючим і навпаки, що міститься в джерелах права або угоді сторін і тягне за собою певні юридичні наслідки [30]. Або, на думку Є.С. Данилової, "юридична фікція – це універсальний прийом юридичної техніки, що використовується у виняткових випадках на стадіях правотворчості і правозастосування, сенсом якого є визнання існуючим свідомо не існуючого факту або навпаки, володіє імперативністю і виконує роль юридичного факту в ситуації непоправної невідомості" [13].

Такий підхід до формування юридичних фікцій розділяється і Р.К. Лотфуліним, який вважає, що "юридична фікція – засіб юридичної техніки, який умовно визнає завідомо неправдиве положення істиною, можливість спростування якої, як правило, не має ніякого юридичного значення" [23].

Вельми цікаві погляди Петражицкого Л.І про фікції [25], коментує Е.В. Тимошина: "існування фікціонної теорії, вважав правознавець (Петражицкий Л.І. – *Авт.*), є прямий наслідок натуралізації і матеріалізації соціальної реальності, а саме помилкового уявлення про суб'єкта права як про вміщеного у простір "тіла", "організму" або "речі" – неможливість виявлення "тіла" юридичної особи тягне за собою необхідний висновок про фіктивний характер даного суб'єкта права". Очевидна непослідовність такої позиції в даному випадку полягає в тому, що фіктивний характер приписується лише одному виду колективних суб'єктів права – юридичним особам, в той час як, підкреслював Л.І. Петражицький, і "місто, держава, лікарня тощо є ніщо, що насправді не існують, якщо розуміти під "дійсним існуванням" його доступність емпіричному спостереженню" [29].

Про подібні ризики несистемного підходу до формування юридичних положень, які базуються на фікції, попереджає О.В. Малько, стверджуючи, що як із сукупності аксіом, так і з сукупності юридичних фікцій не може бути винятків [24]. Іншими словами, зміст юридичної фікції як істинного твердження в правовій системі не може піддаватися сумніву ні в яких особливих випадках. Виходячи з цього, умови, за яких фікція буде сприйматись як юридично вірне твердження повинні бути чітко і вичерпно описані, щоб не допускати неоднозначного трактування.

Інші автори незмінно пов'язують юридичну фікцію з законодавством, оскільки вважають, що вона – це навмисно створене правотворчим органом незаперечне положення, яке може не відповідати дійсності і яке імперативно міститься в нормах права з метою викликання певних правових наслідків [18] .

Деякі дослідники пишуть про використання юридичної фікції у всіх без винятку галузях права, відзначаючи при цьому, що вона ще з часів римського права міцно увійшла в правову традицію як юридико-технічний прийом і найважливіший (можна сказати, імпліцитно притаманний праву) структурний елемент права, а також стверджуючи, що "за підрахунками" цивілістів, більше половини норм цивільного процесу побудовано на фікції [35].

Вважаючи, що юридико-технічний підхід до розуміння значення юридичної фікції применшує її значення для системи права, принципово поділяємо думку про те, що її застосування поза чисто технічними аспектами законодавства в якості своєрідних програмуючих норм, які визначають цілі на перспективу і встановлюють в якості типового або єдино можливого варіанту явно нестандартний для існуючої ступені розвитку суспільства зміст врегульованих правовідносин [17]. Слід тільки зауважити, що, на нашу думку, роль "програмування" правового регулювання в теорії права відведена нормам-принципам.

Розуміючи сутність фікції як твердження того, що суперечить дійсності, тобто того що вона є брехнею, слід все-таки пояснити, заради якого "порятунку" та в ім'я чого це робиться. Які мотиви таких дій, які дозволяють поставити в "топ-режим" поняття моралі в частині сприйняття брехні?

Цікавий варіант мотивації введення юридичної фікції запропонував В.О. Лобовіков: "неминучий відступ від фактичної істини вибачається (виправдовується) "крайньою необхідністю" такого відступу для здійснення значно ціннішої діяльності. Якщо повнота системи є позитивна цінність, то якщо ця цінність значно перевершує цінність якоїсь дріб'язкової істини, цієї дріб'язковою істиною можна пожертвувати заради повноти системи" [22].

Можна погодитися з В.Н. Пяткіним в тому, що правова фікція вводиться для досягнення суспільно-корисних цілей [26]. Більш системно підходить В.І. Червонюк до визначення призначення юридичної фікції, вважаючи, що вона виконує функцію економії правових засобів, що характеризується як юридико-технічний прийом скорочення обсягу законодавства, раціоналізації правової структури, що пристосовує її до правового сприйняття масовою правосвідомістю на набагато кращому рівні ніж без неї [35].

Говорячи про цілі введення юридичних фікцій, К.С. Данилова стверджує, що вони призначені: для усунення невизначеності в правовому регулюванні; допомагають спростити юридичні відносини і зробити правове регулювання стійким і стабільним; скорочують хід і обсяг правової діяльності, полегшують встановлення конкретних обставин і тим самим сприяють процесуальній економії; вносять чіткість і стабільність в правове регулювання, дисциплінують учасників правових відносин, є своєрідним гарантом їх суб'єктивних юридичних прав і свобод [13]. Деякі дослідники вважають, що сучасною тенденцією законодавчого використання фікцій став перехід до технології процесуального регулювання, спрямованої на економію засобів доказування [17].

Підтримуючи необхідність вдосконалення законодавства, що обумовлено багатьма чинниками, А.М. Слюсар стверджує, що сучасна гармонізація законодавства значною мірою пов'язана з удосконаленням юридичної техніки, а тому вважається за необхідне певне переосмислення розуміння і використання окремих її категорій, зокрема, категорії "юридична фікція" [28]. Можна погодитися з таким висновком, але за умови значного розширення як поля цілей гармонізації законодавства, так і поля цілей використання такої категорії як "юридична фікція".

В даний час досить актуальною і необхідною є зміна парадигми формування як окремих правових норм, так і в цілому системи права: необхідно від принципу ретроспективного аналізу і фіксації в правових нормах вже сформованих найбільш стійких суспільних зв'язків і відносин здійснити перехід до принципу створення правових норм, які формують майбутні суспільні відносини на основі наукових прогнозів розвитку соціуму і правових моделей регулювання суспільних відносин майбутнього. Передбачається, що реалізація цієї парадигми з урахуванням очікуваного широкого використання в суспільстві результатів 4-ї науково-технічної революції, в тому числі досягнень IP, штучного інтелекту, нано- та біо- технологій, генетики та генної інженерії, робототехніки тощо, матиме наслідком необхідність перегляду багатьох положень традиційної системи права, в тому числі, пов'язаних з категорією "юридична фікція".

Процитовані вище дефініції терміну "юридична (правова) фікція", і не тільки, містять цілу розсип інших понять, що вживаються різними авторами для позначення одного і того ж явища (юридична фікція) феномена (правова система). Безперечно, таке розмаїття дефініцеутворюючих термінів свідчить про те, що явище "юридична фікція" як

досить складне вивчається вченими в різних аспектах, які для конкретного дослідника є (здаються) найбільш важливими і вагомими.

Як приклад можна навести те, як дослідниками розуміється сутність юридичної фікції. Юридична фікція – це "помилкове положення", "помилкове судження", "те, чого немає в реальності", "неіснуюче положення" , "яке може не відповідати дійсності" тощо. Слова, що при цьому використовуються, мають негативну конотацію, що формує на підсвідомому рівні підозріле ставлення до правових конструкцій, які використовують юридичну фікцію, незважаючи на весь позитив, який вони привносять в систему права.

Крім того, досить часто ми маємо справу в цих дефініціях з такими категоріями як: "реальність", "дійсність", "дійсність, яка не має реального змісту" , "існування" тощо. Але реальність може розумітися як об'єктивна, так і суб'єктивна, яка з них мається на увазі? Дійсність – може розумітися як об'єктивна реальність, тобто існуюча поза залежності від відчуття людини, або як здійснена (матеріалізована) реальність тощо.

Звісно ж, що легкість, з якою ми намагаємося використовувати глибокі за змістом філософські категорії, навколо деяких з яких філософи все ще продовжують дискусії, при визначенні терміну "юридична фікція" може привести і призводить до неоднозначного розуміння змісту цього терміну, а значить і до неоднозначного його використання в процесі правотворчості і до неоднозначного подальшого тлумачення в правозастосуванні.

Багато з досліджуваних термінів не містять визначення мети введення такого явища в системі права як "юридична фікція". Це суттєво послаблює можливості правильного формування правосвідомості та праворозуміння юристів в частині необхідності і доцільності запровадження категорії "фікція" в систему права та подальшого її використання.

Виходячи з вищесказаного, сформулюємо таку дефініцію терміну: ***юридична фікція*** *– це юридична догма, яка дозволяє давати правову характеристику суб'єктам , об'єктам і/або змісту правовідносин на засадах правової аналогії (правової еквівалентності) з іншими змістовно не пов'язаними елементами системи права, та яка використовується суворо в рамках вичерпно визначених правових умов та обмежень її застосування.*

Відомо, що *догма* (від грецького – думка, рішення, вчення, постанова) – це доктрина або окремі її положення, що приймаються за істину без доказів, дослідного обґрунтування і практичної перевірки, а лише на основі релігійної віри чи сліпого підпорядкування авторитету [31].

З врахуванням цього дамо наступне визначення: ***юридична догма*** *– це будь-який елемент системи права або окремі її положення, що приймаються за істину без доказів, дослідного обґрунтування і практичної перевірки, а лише на основі включення їх в правові доктрини або законодавство.* Теоретично до юридичної догми може бути віднесений будь-який елемент права, але найбільш поширені – це норма і інститут права.

Слід звернути увагу на співвідношення термінів "юридична догма" і "догма права".

Досить лаконічне і вичерпне тлумачення останньому терміну дав С.С. Алексєєв, який писав, що "догма права" позначає твердість і незаперечність самої основи, відповідно до якої вирішуються всі юридичні питання, іншими словами, вираз "догма права" в області юридичної діяльності і знань означає те, що об'єктивне (позитивне) право (система позитивного права – *Авт.*), що існує в даному суспільстві, в кожен даний момент – це "те, що є" – строго визначена "даність" і "незмінність" [1, с. 13].

Таким чином, "юридична догма" (норма або інститут прав) і "догма права" (система позитивного права) співвідносяться один з одним як філософські категорії одиничне і загальне.

На основі отриманих результатів досліджень, сформулюємо сукупність цілей введення юридичної фікції. Отже, юридична фікція як елемент системи права призначена для:

– забезпечення своєчасності реакції на виклики певних змін в соціумі в частині необхідності розвитку правової системи;

– усунення невизначеності у правовому регулюванні суспільних відносин, що виникає у зв'язку з інноваціями в житті соціуму, наприклад, з широким використанням нових досягнень 4-й науково-технічної революції, в тому числі досягнень ІР, штучного інтелекту, нано- и біо- технологій, генетики та генної інженерії , робототехніки тощо;

– забезпечення гармонізації правових положень різних галузей права в процесі їх конвергенції, необхідність якої обумовлюється наростаючою появою комплексних складних, багатогранних, часто, нетрадиційних, об'єктів правовідносин;

– створення правових умов для максимального використання напрацьованого століттями багажу знань, досвіду, прийомів і навичок традиційної системи права в умовах реформування законодавства;

– створення умов прозорості, стабільності та стійкості формування системи права;

– економії правових засобів, скорочення обсягу законодавства, раціоналізації структури системи права.

Розвиваючи думку І.В. Філімонової, зауважимо, що назріла актуальність не тільки припущення про можливість визнання [30], але більшою мірою актуальність проведення широких і фундаментальних досліджень поняття "юридична фікція" як категорії юридичної науки і затвердження положень про неї як доктринальних.

Для усунення невизначеності у правовому регулюванні суспільних відносин, пов'язаних з наданням послуг або проведенням робіт на основі застосування технологій ІР з ШІ з частковою участю або зовсім без участі людини, для економії правових засобів, раціоналізації структури системи права, для створення умов наступності з традиційною системою права і для скорочення обсягу законодавства розглянемо можливість і умови введення юридичної фікції.

Для проблеми, яка досліджується в роботі, визначення правових основ регулювання надання послуг і проведення робіт з використанням технологій ІР з ШІ за участю або без безпосередньої участі людини сформулюємо зміст юридичної догми. В даному випадку, юридична догма: система ІР з ШІ, яка виконує частину функцій людини в процесі надання послуг або проведення робіт, визнається традиційним суб'єктом правовідносин в рамках виконання конкретно визначеної діяльності як вичерпної сукупності конкретних дій у встановлених граничних умовах їх здійснення.

Отже, ***юридична догма:*** *система ІР з ШІ, яка виконує частину функцій людини в процесі надання послуг або проведення робіт, є суб'єктом права.*

Тоді для цього випадку, ***юридична фікція***: *система ІР з ШІ як суб'єкт права, може розглядатися в якості представника в розумінні ст. 237 ЦКУ, який зобов'язаний або має право вчиняти правочини від імені її власника (розпорядника), якого вона (система) представляє.*

Або іншими словами, приймається, що система ІР з ШІ – це представник суб'єкта права в розумінні статті 237 ЦКУ, оскільки вона зобов'язана або має право вчиняти дії від імені суб'єкта права і суто в його інтересах в межах наділених повноважень, що визначається алгоритмами її комп'ютерної програми.

Змістом запропонованої юридичної фікції є твердження того, що юридичні статуси традиційного представника суб'єкта права і системи ІР з ШІ як "представника" суб'єкта права є однаковими. З цього твердження випливає, що як система ІР з ШІ, так фізичні і

юридичні особи, при виконанні повноважень представника суб'єкта права, мають однакові (еквівалентні) цивільні права і обов'язки.

Припущення щодо еквівалентності цивільних прав та обов'язків "системи ІР" і "представника" має наступні підстави. Права і обов'язки представника суб'єкта права, які відображаються в договорі про представництво, вичерпно визначають зміст його дій. З іншого боку, зміст дій системи ІР з ШІ вичерпно визначаються алгоритмом її дій, який задається за допомогою комп'ютерної програми, зміст якої можна визнати визначенням прав та обов'язків системи ІР з ШІ, як представника суб'єкта права. І в першому, і в другому випадку зміст дій представника суб'єкта права будуть одні і ті самі, оскільки вони однаково регламентовані або договором, або алгоритмом дій, який визначається комп'ютерною програмою.

Умовність припущення щодо еквівалентності цивільних прав та обов'язків фізичної (юридичної) особи і системи ІР з ШІ як представників не має значення для суб'єктів права, оскільки, з точки зору реального задоволення їхніх прав і інтересів результати дій цих різних представників будуть еквівалентними.

Запропонована юридична фікція, що базується на юридичній догмі про визнання наявності у систем ІР з ШІ цивільної правосуб'єктності строго в рамках договору про представництво, дозволить задіяти весь вже наявний арсенал правових механізмів, напрацьований наукою і практикою, з метою правового регулювання суспільних відносин, пов'язаних з використанням технологій ІР з ШІ при наданні послуг або проведенні робіт з участю або зовсім без участі людини.

Таким чином, для гібридних правовідносин, в яких на основі договору, закону, акту органу юридичної особи та з інших підстав, встановлених актами цивільного законодавства, буде використовуватися запропонована юридична фікція, їх зміст буде визначатися правовим регулюванням відповідно до положень класичної теорії цивільного права в частині представництва.

Теоретичні та правові проблеми, що мають місце в разі укладення і виконання договорів представництва між суб'єктами права, в умовах запропонованої юридичної фікції будуть поширюватися і на випадки представлення інтересів і прав суб'єкта системою ІР з ШІ. У різних державах все ще триває жвава наукова дискусія з приводу з'ясування правової природи представництва, визначення правових режимів, що регулюють цю діяльність, особливостей прав, обов'язків і відповідальності суб'єктів договору представництва [14]. До речі, Цивільний кодекс Франції (стаття 739) встановлює, що представництво є юридичною фікцією, яка має на меті допустити вступ в права того, кого він представляє [11].

Для технологій ІР, які за своєю природою є транскордонними, досить типовими будуть випадки, коли суб'єкти суспільних відносин, що реалізуються за їх допомогою, будуть відноситись до різних національних юрисдикцій. При цьому підкреслюється, що договори представництва важко буде привести до єдиного знаменника в зв'язку з різним тлумаченням сутності цього договору в правовій теорії і практиці різних держав, оскільки існуючі в різних країнах інститути представництва виконують одну і ту ж економічну функцію, але мають неоднакову правову природу [16].

У майбутньому для випадку використання технологій ІР цілком вірогідні ситуації, коли в правовідносинах буде брати участь велика кількість суб'єктів різної національної юрисдикції. Більш того, в умовах динамічності процесів, пов'язаних з використанням технологій ІР з ШІ, стануть поширеними каскадні правовідносини, тобто послідовний ланцюжок правовідносин, в яких об'єктом кожного наступного правовідношення буде

результат реалізації попереднього правовідношення. При цьому суб'єкти цих правовідносин також можуть відноситись до різних національних юрисдикцій.

Тому уявляється досить актуальною організація досліджень щодо можливості розробки і прийняття міжнародно-правового акту, який би уніфікував підходи до правового регулювання правовідносин, пов'язаних з виконанням функцій представництва системами ІР з ШІ в інтересах суб'єктів права різної національної юрисдикції.

Висновки.

1. У світі лавиноподібно зростають приклади та обсяги використання технологій Інтернету речей з штучним інтелектом в різних сферах суспільної активності, що в певних випадках призводить до виникнення правової невизначеності, наявність якої обумовлює актуальність визначення теоретико-правових засад регулювання надання послуг і проведення робіт з застосуванням систем IoT з ШІ за участю і без безпосередньої участі людини.

2. За результатами дослідження правових моделей надання послуг за допомогою систем Інтернету речей з штучним інтелектом запропоновані моделі правовідносин, введено поняття безпосередніх, опосередкованих та гібридних правовідносин, що дозволяє виявити та врахувати в подальшому правовому аналізі особливості впливу застосування цих систем на суспільні відносини.

3. З детального аналізу безпосередніх і опосередкованих правовідносин випливає можливість зробити припущення про те, що юридичні наслідки дій систем ІР з ШІ є тотожними юридичним наслідкам аналогічних дій традиційного (в юридичному сенсі) представника.

4. Для вивчення особливостей суспільних відносин в процесі надання послуг та проведення робіт запропоновані визначення робастного та детермінованого соціального управління, що дозволило довести функціональну аналогію поведінки системи ІР з ШІ та суб'єкта при здійсненні однієї і тієї самої певної діяльності.

5. Сформульовані дефініції категорії "юридична догма" "юридична фікція" створили підґрунтя для усунення невизначеності у правовому регулюванні суспільних відносин, пов'язаних з інноваціями в житті соціуму, наприклад, з широким використанням нових досягнень 4-й науково-технічної революції, в тому числі досягнень технологій ІР, штучного інтелекту, нано- та біо-технологій, генетики та генної інженерії, робототехніки тощо.

6. Запропоновано юридичні новели:

– в якості юридичної догми: *система ІР з ШІ, яка виконує частину функцій людини в процесі надання послуг або проведення робіт є суб'єктом права*, тобто система ІР з ШІ, яка виконує частину функцій людини в процесі надання послуг або проведення робіт, беззаперечно визнається традиційним суб'єктом правовідносин в рамках виконання конкретно визначеної діяльності як вичерпної сукупності конкретних дій у встановлених граничних умовах їх здійснення;

– в якості юридичної фікції: *система ІР з ШІ як суб'єкт права, може розглядатися в якості представника в розумінні ст. 237 ЦКУ, який зобов'язаний або має право вчиняти правочини від імені її власника (розпорядника), якого вона (система) представляє*, тобто юридичні статуси традиційного представника суб'єкта права і системи ІР з ШІ як "представника" суб'єкта права є однаковими, зокрема, вони мають однакові (еквівалентні) цивільні права і обов'язки.

7. Введення в систему права та законодавства запропонованої юридичної фікції, що базується на юридичній догмі, про визнання наявності у систем ІР з ШІ цивільної

правосуб'єктності строго в рамках договору про представництво, дозволить задіяти весь вже наявний арсенал правових механізмів, напрацьований наукою і практикою, для забезпечення правового регулювання суспільних відносин, пов'язаних з застосуванням технологій Інтернету речей з штучним інтелектом при наданні послуг або проведенні робіт з участю або зовсім без участі людини.

Використана література

1. Алексеев С.С. Восхождение к праву. Поиски и решения. Москва: НОРМА, 2001. 752 с.
2. Афанасьев В.Н. Управление неопределенными динамическими объектами. Москва: ФИЗМАТЛИТ, 2008. 208 с.
3. Баранов О.А. Інтернет речей (IoT): правові проблеми застосування розумних контрактів. *Інформація і право*. № 4(23)/2017. С. 26-40.
4. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.
5. Баранов О.А. Інтернет речей і штучний інтелект: витоки проблеми правового регулювання: зб. матеріалів II-ї міжнародної науково-практичної конф. *IT-право: проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ "Львівська політехніка", 2017. 318 с. С. 18-42.
6. Баранов О.А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. I. Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія. 2-ге вид. Харків: Право, 2018. 344 с.
7. Бекбаев Е.З. Проблема начала в теоретическом познании правовой системы (попытка обоснования) стана. 2008 г. 296 с. URL: http://www.allpravo.ru/library/doc108p0/instrum7129/print 7135.html (дата звернення: 7.12.2018).
8. Вандыш-Бубко В.В., Гиленко М.В. Когнитивные расстройства в судебно-психиатрической практике. *Доктор.ру*. 2013. № 5(83). С. 86-92.
9. Варшавский Л. Е. Моделирование динамики экономических систем с неопределенными параметрами. Компьютерные исследования и моделирование, 2018. Т. 10. Вып. 2. С. 261-276. URL: http://www.mathnet.ru/php/archive.phtml?wshow=paper&jrnid=crm&paperid=164&option _lang =rus (дата звернення: 7.12.2018).
10. Винер Н. Кибернетика, или управление и связь в животном и машине / пер. с англ. И.В. Соловьева и Г.Н. Поварова / под ред. Г.Н. Поварова. 2-е изд. Москва: Наука (Главная редакция изданий для зарубежных стран). 1983. 344 с.
11. Гражданский кодекс Франции (Кодекс Наполеона) / пер. с франц. В.Н. Захватаев / отв. ред. А.С. Довгерт. Киев: Истина, 2006. 1008 с.
12. Давыдова М.Л. Юридическая техника: проблемы теории и методологии: монография. Волгоград: ВолГУ, 2009. 318 с.
13. Данилова Е.С. К вопросу о понятии, классификации и значении юридических фикций. *Юридическая наука*. 2014. № 3. С. 112-118.
14. Дороженко М. Ю. Гражданско-правовое регулирование представительства: проблемы теории и законодательства: автореф. дис. …канд. юрид. наук: 12.00.03. Москва, 2007. 26 с. URL: http://law.edu.ru/book/book.asp?bookID=1274648 (дата звернення: 7.12.2018).
15. Бабкина Е.В. Правовое регулирование договоров агентирования и дистрибьюции в европейском праве. *Труды факультета международных отношений*. 2014. Вып. 4. С 93-96.
16. Бабкина Е.В. Правовая природа договора коммерческого представительства. *Белорусский журнал международного права и международных отношений*. 2000. № 2. URL: http://evolutio.info/content/view/353/51 (дата звернення: 7.12.2018).
17. Зеленко І.П. Юридична фікція як правовий та соціальний інструмент. *Науковий вісник Ужгородського національного університету*. 2013. Вип. 23. Ч. I. Т. 1. С. 46-49.
18. Ишигилов И.Л. Понятие юридических фикций. *Сибирский юридический вестник*. 2007. № 1. С. 3-7.

19. Как Big Data помогает Walmart продавать на полтриллиона долларов в год: Skywell. URL: http://www.skywell.com.ua/blog/kak-big-data-pomogaet-walmart-prodavat-na-poltrilliona-dollarov-v-god (дата звернення: 7.12.2018).

20. Кечекъян С.Ф. Правоотношения в социалистическом обществе. Москва, 1958. 188 с. URL: http://www.pravo.vuzlib.org/book_z622_page_28.html (дата звернення: 7.12.2018).

21. Трофимова Л.А., Трофимов В.В. Управленческие решения (методы принятия и реализации). Санк-Питербург: СПбГУЭФ, 2011. 190 с. URL: http://economics.studio/mened jmenta-voprosyi-obschie/upravlencheskie-resheniya-metodyi-prinyatiya.html (дата звернення: 7.12.2018).

22. Лобовиков В.О. Проблема неполноты формально определенных систем норм позитивного права, первая теорема Гёделя о неполноте и юридические фикции как важный компонент юридической техники. *Научный вестник Омской академии МВД России*. 2013. № 2(49). С. 53-57.

23. Лотфуллин Р.К. Юридические фикции в гражданском праве. Москва: Юридическая литература, 2006. 213 с.

24. Малько А.В., Роман Е.А. Исключения в праве и правовые фикции: технико-юридический аспект. *Право и управление. XXI век*. 2015. № 4. С. 15-19.

25. Петражицкий Л.И. Очерки философии права. Теория и политика права. Изб. труды / под ред. Е.В. Тимошиной. Санк-Петербург, 2010. 370 с.

26. Пяткин В. Н. Содержание и соотношениепонятий “правовая фикция” и “фиктивная норма”. *Социально-политические науки*. 2012. № 4. С. 41-44.

27. Саймон Г.А. Теория принятия решений в экономической теории и науке о поведении / пер. И.В. Попович. С. 54-72. Теория фирмы / под ред. Гальперина. Санк-Петербург: Экономическая школа, 1995. (Вехи экономической мысли). Вып. 2. 534 с. URL: http://portalus.ru/modules/economics/rus_readme.php?subaction=showfull&id=1102951561&archive=1120044309&start_from=&ucat=& (дата звернення: 7.12.2018).

28. Слюсар А.М. Щодо питання юридичних фікцій у трудовому праві. *Право та інновації*. 2016. № 1(13). С. 33-34.

29. Тимошина Е.В. Право как “идея”, как “фикция” и как “факт”: о номинализме и реализме в теории права. *Труды Института государства и права Российской академии наук*. 2013. № 4. С. 48-75.

30. Филимонова И.В. Понятие, сущность, признаки и значение юридической фикции: мат. международной научно-практической конференции *Понимание государства и права. Подходы и проблемы*, 8 июня 2013. Пятигорск: Рекламно-информационное агентство на Кавминводах, 2013. С. 142-150.

31. Философский энциклопедический словарь / гл. редак.: Л.Ф. Ильичёв, П.Н. Федосеев, С.М. Ковалёв, В.Г. Панов. Москва: Советская энциклопедия, 1983. 840 с.

32. Халфина Р.О. Общее учение о правоотношении. Москва: Юридическая литература, 1974. 340 с. URL: http://www.pravoznavec.com.ua/books/3/101/17/#chapter (дата звернення 7.12.2018).

33. Харазов В.Г. Интегрированные системы управления технологическими процессами: справочник. Москва, 2009. 550 с.

34. Харитонов Э.О. Становлення інституту представництва у цивільному законодавстві України. *Міжнародний юридичний вісник*: зб наукових праць Національного університету державної податкової служби України. Вип. 1(1). 2014. С. 170-176. URL: http://asta.edu.ua/files/Files/vicnyk/Harytonov.pdf (дата звернення: 7.12.2018).

35. Червонюк В.И. Структура права: закономерности формирования и развития: в 9 вып. Вып. 5. Логический инструментарий права. *Вестник Московского университета МВД России*. 2014. № 4. С. 162-168.

36. Bolen A. Internet of Things examples from 3 industries: SAS. URL: https://www.sas.com/en_us/insights/articles/big-data/3-internet-of-things-examples.html (дата звернення: 7.12.2018).

37. Dreher A. The Smart Factory of the Future: BELDEN, 28 January 2015. URL: http://www.belden.com/blog/industrialethernet/The-Smart-Factory-of-the-Future-Part-1.cfm (дата звернення 7.12.2018).

38. Lamparter S., Luckner S., Mutschler S. Formal Specification of Web Service Contracts for Automated Contracting and Monitoring. Proceedings of the 40th Annual Hawaii International Conference on System Sciences, 2007. Januar. Verlag: Computer Society Press. URL: https://www.computer.org/csdl/proceedings/hicss/2007/2755/00/27550063b.pdf (дата звернення: 7.12.2018).

39. Manyika J. Disruptive technologies: Advances that will transform life, business, and the global economy. McKinsey Global Institute, 2013. 162 p. URL: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/disruptive-technologies (дата звернення: 7.12.2018).

40. Moglen E. Legal Fictions and Common Law Legal Theory: Some Historical Reflections. 10 Tel Aviv U. Stud. L., 1990. 33. URL: http://moglen.law.columbia.edu/publications/fict.html (дата звернення: 7.12.2018).

41. New app replaces ultrasound with smartphone camera to measure heart health: EurekAlert, 5 Sep. 2017. URL: https://www.eurekalert.org/pub_releases/2017-09/ciot-nar090517.php (дата звернення 7.12.2018).

42. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. Final report of the Industrie 4.0. Federal Ministry of Education and Research, 2013. – P. 78. URL: http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf (дата звернення 7.12.2018).

43. Smart Agriculture Market by Agriculture Type (Precision Farming, Livestock Monitoring, Fish Farming, Smart Greenhouse), Hardware (GPS, Drones, Sensors, RFID, LED Grow Lights), Software, Services, Application, and Geography. Global Forecast to 2022. Research and Markets, 2017. P. 212. URL: https://www.researchandmarkets.com/reports/4143579/smart-agriculture-market-by-agriculture-type#rela9 (дата звернення 7.12.2018).

44. Vermesan O., FriessP. Internet of Things: From Research and Innovation to Market Deployment. River Publishers, 2014. – P. 355. URL: http://www.internet-of-things-research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf (дата звернення 7.12.2018).

45. Wang B. Peak Car Ownership is near – beginning of the fall of car ownership: NEXT BIG FUTURE, 13 March 2017. URL: https://www.nextbigfuture.com/2017/03/peak-car-ownership-is-near-beginning-of.html (дата звернення 7.12.2018).

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

УДК 681.3+314.1:004.6

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

УЗАГАЛЬНЕННЯ ІНДЕКСУ ЦИТУВАННЯ ЯК КОМПЕНСАЦІЯ НЕПОВНОТИ НАУКОМЕТРИЧНИХ БАЗ ДАНИХ

Анотація. *В роботі розглянуті специфічні проблеми сучасної наукометрії, пов'язані з технологією наповнення наукометричних баз даних. Показано, що загальноприйняті методики оцінки виконання наукової діяльності окремими науковцями та організаціями не відповідають повною мірою поставленій меті внаслідок неповноти охоплення наявного масиву наукових публікацій. Запропоновано один із можливих шляхів вдосконалення методики, заснованої на визначенні індексу цитування.*

Ключеві слова: *база даних, індекс цитування, рецензування.*

Summary. *The paper considers the specific problems of modern scientometrics related to the technology of filling scientometric databases. It is shown that the methods commonly used for assessing the performance of scientific activity by individual scientists and organizations do not fully meet the goals set, as a result of the incompleteness of the coverage of an existing array of scientific publications. One of the possible ways to improve the method based on the definition of the citation index is proposed.*

Keywords: *database, citation index, reviewing.*

Аннотация. *В работе рассмотрены специфические проблемы современной наукометрии, связанные с технологией наполнения наукометрических баз данных. Показано, что общепринятые методики оценки выполнения научной деятельности отдельными учеными и организациями не соответствуют в полной мере поставленной цели вследствие неполноты охвата имеющегося массива научных публикаций. Предложен один из возможных путей усовершенствования методики, основанной на определении индекса цитирования.*

Ключевые слова: *база данных, индекс цитирования, рецензирование.*

Постановка проблеми. Вивчення науки як інформаційного процесу [1] на наш час набуває дедалі більшого значення, в першу чергу через те, що результати сучасних наукових досліджень становлять фундамент створення нових технологій. Окреме місце в цьому напрямі становить визначення кількісної міри оцінки виконання наукової діяльності окремими науковцями та організаціями, оскільки від її успішного вирішення залежить ефективність фінансування науки.

Загальноприйнята методика, заснована на визначенні індексу цитування наукових праць, має певні проблеми, пов'язані з технологією наповнення баз даних, що при цьому використовуються.

В роботі пропонується узагальнена кількісна міра наукової ефективності, яка не потребує нових методик отримання додаткових даних, але разом з тим нівелює головні недоліки стандартних наукометричних оцінок.

Результати аналізу наукових публікацій. Критичний аналіз поточної ситуації свідчить про загалом незадовільний стан справ в даній сфері (див., наприклад [2; 7 – 8] і посилання в них). На практиці кореляція між існуючими показниками наукової діяльності та її реальною вагою в плані фактичного розвитку науки залишається відносною та приблизною. Ретроспективний погляд виявляє багато прикладів, коли суттєвий вплив на розвиток певної наукової галузі мали роботи, що отримали посередню оцінку на момент публікації. І навпаки, результати з високими показниками

швидко втрачали актуальність та забувалися науковою спільнотою, не залишивши помітного сліду в подальших дослідженнях. Особливо це характерно для гуманітарних наук, в яких результати досліджень не співставляються з емпіричними даними, через що часто важко визначити їхню реальну наукову вагу.

На нашу думку, в сучасній наукометрії існує дві головні проблеми. Перша полягає в правильній розробці наукометричних параметрів, які адекватно свідчать про рівень наукової діяльності. Другою проблемою є організація баз даних, за допомогою яких здійснюється визначення конкретних значень цих параметрів.

На перший погляд, вони не залежать одна від одної, але насправді тісно пов'язані між собою. Причина полягає в тому, що бази даних фактично створюються під конкретні методики визначення потрібних параметрів, а параметри визначаються таким чином, щоб їхні значення могли бути визначені на практиці. І тут виникають обмеження, що суттєво впливають на ефективність наукометрії.

Метою статті є вдосконалення кількісної міри оцінки наукової ефективності шляхом об'єднання методик визначення індексу цитування за різними базами даних та врахування додаткового покажчика – рівня рецензованості публікацій.

Виклад основного матеріалу. У цій роботі розглядаються дві основні методики оцінки виконання наукової діяльності: цитування та рецензування. Головні проблеми сучасної наукометрії пов'язані саме з методикою цитування [2; 4]. Тому, як вважаємо, спосіб визначення кількісної міри оцінки виконання наукової діяльності може бути вдосконалений шляхом об'єднання цих методик.

Цитування. На наш час основою наукометричною методикою є цитування. Термін "цитування" ми будемо використовувати в широкому розумінні, оскільки існує кілька його різновидів. Але для нас відмінності між ними не є суттєвими, оскільки вони лише по-різному визначають кількісну міру рівня цитованості наукової праці. Тому ми просто говоритимемо про індекс цитування (Science Citation Index – SCI), маючи на увазі, що він може обчислюватись різними способами [2 – 6].

Індекс цитування, безперечно, має багато суттєвих переваг перед іншими наукометричними методиками, але й низку недоліків [2; 7 – 8]. Ми не маємо наміру наводити детальну критику індексу цитування як наукометричної методики. Зосередимось лише на одному аспекті даної проблеми.

Офіційно вважається, що SCI "оцінює вплив вченого або організації на світову науку, визначає якість проведених наукових досліджень" [9]. Але це твердження потребує певних коментарів.

Насправді кількість цитувань наукової праці свідчить не про її безпосередній вплив на світову науку і не про якість проведених наукових досліджень, а про наявність у неї певних характерних рис, які зумовлюють активне використання її в колективній науковій діяльності. І це – серйозна проблема сучасної наукометрії. Реальна оцінка наукової діяльності має більш складний, опосередкований характер.

Наука вже давно не є справою окремих видатних мислителів. Реальні дослідження здійснюються великими колективами фахівців, причому багато з них діють незалежно, взаємно перевіряючи і вдосконалюючи отримані дані. Протягом останніх десятиліть в міжнародній науковій спільноті сформувалися добре визначені способи взаємодії наукових колективів та окремих науковців, які забезпечують ефективне використання досягнень колег. Внаслідок цього були вироблені певні норми представлення наукових результатів, які забезпечують, з одного боку оптимальне сприйняття досягнень авторів, а з другого боку – можливості їх критичної оцінки. Тому дотримання відповідних норм

свідчить про високі шанси того, що отримані результати будуть з належною ефективністю використані іншими дослідниками на світовому рівні.

Колективний характер сучасної наукової діяльності закономірно призвів до формування специфічної технології здійснення досліджень і оформлення їх результатів. І ключову роль в ній відіграє саме SCI, оскільки він є одним з головних чинників при вирішенні низки важливих питань включно з фінансуванням наукової діяльності.

Такий стан справ має і зворотній бік: формування таких механізмів визначення значень SCI, які б забезпечили максимальну ефективність його використання в рамках прийнятої наукометричної парадигми.

Перш за все слід зазначити, що визначення SCI не може здійснюватися безпосередньо людиною – для цього потрібно опрацьовувати надто великі обсяги інформації. Крім того, має бути довіра до тих, хто робить цю справу. Тому були створені спеціалізовані організації, які професійно займаються визначенням SCI і знаходяться під контролем наукової спільноти.

Детально до цього питання ми звернемося нижче, а зараз зазначимо, що технологія ефективного визначення SCI неодмінно впливає на процес охоплення загального масиву результатів наукових досліджень.

Бази даних. В основі технології визначення SCI лежить створення баз даних, які містять дані щодо наявності в бібліографічних списках наукових праць посилань на ті чи інші наукові праці. Технічні питання нас зараз не цікавлять, головне полягає в тому, що наукометричні бази даних (далі – НБД) створюються шляхом опрацювання публікацій наперед визначеного переліку наукових видань. Ця обставина здається цілком очевидною і природною, але вона породжує неочевидні наслідки, які і є темою нашого дослідження.

Спочатку звернемося до поточного стану справ.

На цей час основними є такі бази даних (точніше, комплекси баз даних): Scopus [10], Web of Science [11] та Google Scholar [12].

Scopus – бібліографічна та реферативна база даних, що входить до складу інтегрованого науково-інформаційного середовища SciVerse [13]. Сьогодні Scopus є найбільш потужним і авторитетним інформаційним ресурсом в наукометрії.

Web of Science – платформа, на якій розміщено бази даних наукової літератури і патентів, яка містить в собі інструментальні засоби пошуку, аналізу та управління бібліографічною інформацією.

Google Scholar – пошукова система, яка індексує повний текст наукових публікацій, представлених в усіх форматах. Хоча Google Scholar проектувалася і створювалася саме як пошукова система, вона фактично має досить потужні інструментальні засоби визначення наукометричних параметрів. Зазначимо, що ця система є популярною переважно в колах власне науковців. Одна з причин полягає в тому, що бази даних Google Scholar створюються шляхом індексації всіх відкритих джерел в мережі Інтернет, без жодних редакційних обмежень. Але для офіційного визначення SCI не використовується.

Зазначимо, що Scopus і Web of Science індексують лише джерела, які мають імпакт-індекс.

Оскільки основним інформаційним ресурсом в сучасній наукометрії є Scopus, зупинимося на цій системі детальніше. Нас цікавитиме два моменти: структура баз даних та механізми їх наповнення.

Структура Scopus містить три основні категорії наукометричних даних: профілі авторів, профілі організацій, профілі джерел. Отже, система дозволяє отримувати досить широкий спектр даних, в тому числі і таких, що стосуються безпосередньо авторів. Що само по собі має як позитивні, так і негативні наслідки.

Дані розміщуються у відповідності з класифікаційною системою SciVerse Scopus, яка включає 24 тематичні розділи [14], поділених на 335 підрозділів. Розділи мають дворівневу таксономію:

1. Фізичні науки.
   1.1. Хімічні технології.
   1.2. Хімія.
   1.3. Комп'ютерні науки.
   1.4. Науки про Землю та планети.
   1.5. Енергетика.
   1.6. Виробництво.
   1.7. Матеріалознавство.
   1.8. Математика.
   1.9. Фізика і астрономія.
2. Медичні науки.
   2.1. Медицина та стоматологія.
   2.2. Сестринська справа та медичні професії.
   2.3. Фармакологія, токсикологія та фармацевтичні науки.
   2.4. Ветеринарна справа та ветеринарна медицина.
3. Науки про життя.
   3.1. Сільськогосподарські та біологічні науки.
   3.2. Біохімія, генетика та молекулярна біологія.
   3.3. Науки про навколишнє середовище.
   3.4. Імунологія та мікробіологія.
   3.5. Нейронауки.
4. Соціогуманітарні науки.
   4.1. Мистецтвознавчі та гуманітарні науки.
   4.2. Бізнес, менеджмент та бухгалтерський облік.
   4.3. Теорії прийняття рішень.
   4.4. Економіка, економетрика та фінанси.
   4.5. Психологія.
   4.6. Соціальні науки.

Вже на рівні тематичних розділів видно, що класифікація є не надто розвинена. До цього питання ми повернемося нижче.

Наповнення баз даних Scopus здійснюється шляхом індексації джерел за запитами. Індексуються наукові журнали, матеріали конференцій та серіальні книжкові видання.

Рішення про індексацію приймаються Консультативним комітетом Scopus з відбору змісту (CSAB). До цього комітету входять галузеві фахівці, які представляють різні галузі науки та різні регіони світу. Запити на включення нового джерела можуть подаватися як вченими, так і членами CSAB. Рішення про включення нових джерел приймаються щорічно.

Незважаючи на певні слабкості, така система виглядає на перший погляд цілком прийнятною. Та більш глибокий аналіз свідчить, що з точки зору наукометрії вона має суттєві недоліки.

Отже, під переліком джерел НБД ми розуміємо весь вміст описаних вище баз даних, але говоритимемо про бази даних Scopus як найбільш вживаних в сучасній наукометрії.

Безперечно, до переліку джерел НБД входять провідні фахові видання, в яких друкуються видатні вчені. Поза всяким сумнівом, праці, надруковані в цих виданнях, з

високою імовірністю впливають на розвиток науки. Тому посилання, що містяться в таких публікаціях, дійсно свідчать про актуальність відповідних праць в середовищі активно працюючих науковців.

Але обсягів провідних видань не вистачає для публікації всіх результатів наукових досліджень. Через це частина наукових праць неминуче видається в менш престижних виданнях. А це означає, що публікація в "другорядному" виданні не обов'язково має низький науковий рівень – для неї просто не вистачило місця в провідному виданні.

Таким чином, для побудови повної НБД необхідно включити до переліку всі видання (тобто мають враховуватися всі цитування). Але це на наш час фізично неможливо. Отже, маємо принципово неповний набір даних, на основі якого визначається SCI. Підкреслимо, що ця неповнота зумовлена суто технологічними чинниками. Головними з них є два: складність обробки великих масивів даних (а в цьому випадку вони дійсно великі, оскільки цитування визначається не менш, ніж двома наборами даних, і відповідні витрати ресурсів зростають принаймні в квадраті), і отримання потрібних даних. Щодо першого, можемо сподіватися, що технічний прогрес дозволить збільшити обсяги даних, доступні для машинної обробки, а з другим ситуація складніша. Дані можуть бути отримані лише з видань, які надають тексти публікацій у відкритому доступі. Тому до переліку завідомо не потрапляють видання з обмеженим доступом (в яких друкуються матеріали, що мають гриф секретності), і цитування в них звичайних публікацій з відкритих джерел не враховуються. Також слід враховувати фактор часу: в багатьох виданнях існує черга, і багато публікацій, що містять посилання на дану працю, не потрапляють до переліку просто тому, що не встигли вийти в друк на момент чергового оновлення НБД.

Оптимізація технології формування переліку видань для НБД, свідомо чи ні, призводить до надання переваги тим із них, які характеризуються максимальною концентрацією взаємних (по відношенню до самих джерел) цитувань. На практиці це означає, що в НБД в першу чергу реєструються видання, тематика яких охоплює найбільш актуальні напрямки досліджень в світовому контексті. Таким чином, значна кількість видань лишається не опрацьованою, а отже, і не врахованою при визначенні SCI. Підкреслимо: ця обставина зумовлена не хибною політикою організацій, які створюють і експлуатують НБД, а суто технологічними чинниками. Зазначимо також, що окремою проблемою є небажання або неможливість (з тих чи інших причин) редакцій деяких видань реєструватися в НБД.

Отже, маємо подвійну обмеженість оцінки рівня цитованості: в процесі його визначення можуть ігноруватися як самі публікації (для них SCI дорівнює нулю, хоча насправді вони можуть мати непогані показники), так і частина посилань на них.

Проблема індексу цитування в українській науці. Проблема принципової неповноти НБД зумовлює зворотній вплив на процес публікацій наукових праць. У науковців виникає концептуально важлива потреба друкуватися лише у виданнях, що входять до НБД. А це, на жаль, далеко не завжди можливо.

Найбільш типовою причиною є відсутність в переліку видань НБД відповідних наукових напрямків.

Класифікаційна система SciVerse Scopus, як ми вже бачили, досить загальна, щоб реально відбивати тематичну різноманітність сучасної науки. Так, наприклад, дослідження з загальної теорії систем може, очевидно, класифікуватися за розділами "Комп'ютерні науки" або "Математика", але це, строго кажучи, неправильно. Існує розділ "Теорії прийняття рішень", хоча такої науки, власне кажучи, взагалі не існує. Натомість відсутній розділ під орієнтовною назвою "Історичні науки". До якого розділу

слід віднести етнографію та етнологію? І чи повинні вони належати до одного розділу, чи до різних? Правові науки формально повинні відноситися до розділу “Соціальні науки”, але заздалегідь не відомо, чи проіндексовані в цьому розділі видання, які приймуть до друку працю на тему сучасного українського законодавства. Загалом, це типова ситуація для штучно побудованих класифікаційних систем: вони виявляються або надто громіздкими, або недостатньо гнучкими в практичному використанні. Часто вчений, незалежно від свого реального рівня, просто не має, куди надіслати свою працю, щоб для неї був визначений SCI.

Але навіть за наявності відповідного розділу та підрозділу, існує поширена проблема відмов у публікації редакцій журналів. На жаль, українські вчені регулярно отримують недостатньо мотивовані відмови, як правило з посиланням на “погану англійську мову”. При чому таку відмову отримують шановані фахівці, які не мають проблем у спілкуванні англійською мовою з зарубіжними колегами на міжнародних конференціях, семінарах, школах тощо.

Справжня причина, наскільки можемо судити, полягає в тому, що вітчизняні науковці здобували освіту і виховувалися як вчені на базі радянських стандартів здійснення наукових досліджень і оформлення їх результатів. А вони радикально відрізняються від стандартів, прийнятих в міжнародній науковій спільноті [15]. Рецензенти та редактори зарубіжних видань усвідомлюють, що стаття написана не так, як мала б бути, але не володіють адекватними засобами артикуляції. Тому наводиться формальна причина відмови, часто необґрунтована.

Це є серйозна проблема для вітчизняних науковців, оскільки загальною практикою стала вимога адміністрацій наукових установ друкувати результати своїх досліджень у виданнях, що входять до переліку НБД, в першу чергу баз даних Scopus.

На перший погляд, ситуація може бути вирішена шляхом створення української НБД, яка б розширила перелік НБД таким чином, щоб до нього були включені вітчизняні джерела. І останнім часом в Україні розпочалася підготовка до створення національної НБД [16 – 18]. Звичайно, цю ініціативу можна лише вітати. Але вона сама по собі не вирішує всі проблеми.

На наш погляд, ефективне вирішення проблеми має бути комплексним і містити в собі принаймні два важливі напрямки: розширення НБД і вдосконалення наукометричних показників. Ця проблема не є суто українською, вона актуальна і в багатьох інших країнах. Тому наші пропозиції можуть виявитися цікавими і корисними в широкому суспільному контексті.

Розширення НБД може бути практично застосовано шляхом врахування як міжнародних НБД, так і національних. Тобто, в найпростішому варіанті можемо визначати суму міжнародного та вітчизняного SCI. Більш того, міжнародний SCI можна розширити за рахунок усереднення даних Scopus та Web of Science. Складові можуть братися з належним чином визначеними ваговими множниками. Очевидно, що така методика не призведе до втрат в оцінці результатів досліджень – кінцеве значення може лише збільшитися за рахунок розширеного масиву даних.

Але таке розширення баз даних не вирішує проблему в цілому, тому що лишається невизначеність щодо рівня вагомості цитувань. Однакові значення SCI, отримані на основі міжнародних та національних НБД, світова наукова спільнота не визнає рівноцінними. Дивлячись на отримане конкретне число, ми не можемо визначити, які НБД дали в нього основний внесок. В такий спосіб неможливо відрізнити науковця високого рівня, який не має публікацій в НБД Scopus через зазначені вище причини, від науковця, який не має таких публікацій через власний низький рівень. Отже,

прямолінійне розширення НБД слід доповнити додатковими факторами, які могли б компенсувати його недоліки.

На нашу думку, таким фактором могла б бути кількісна міра рівня рецензованості (якщо можна так сказати) наукових праць.

Строго кажучи, рецензування як таке не відноситься до сфери наукометрії, оскільки не передбачає визначення того чи іншого параметра, що має кількісну міру. Але з роками воно все ширше використовується при оцінці роботи науковців, а отже на функціональному рівні вирішує ті ж задачі, що й наукометрія. Більше того, існує думка (див., наприклад [2]), що рецензування може розглядатися як альтернатива формалізованим методам наукометрії в класичному розумінні цього слова. Така точка зору, безперечно, має сенс. Але ми пропонуємо дещо інший підхід: ввести на його основі додатковий параметр.

Фахові видання поділяються на рецензовані та нерецензовані. В рецензованих виданнях може бути опублікована лише праця, яка пройшла рецензування незалежними експертами. Процедура рецензування, як і будь-яка інша, має свої недоліки. Але не викликає сумніву те, що фаховий рівень рецензованих наукових праць в середньому вищий, ніж нерецензованих.

Важлива перевага рецензування як критерію оцінки наукового рівня полягає в тому, що воно ніяк не залежить від жодних тематичних класифікацій. Редакція сама вибирає рецензентів, і якщо праця науковця написана на актуальну тему, обов'язково знайдуться інші фахівці в тій же галузі досліджень. У випадку належного фахового рівня праця отримає позитивну рецензію. І навпаки, результати дослідження, виконаного на низькому рівні, не пройдуть рецензування навіть за тематичної належності до наукового мейнстріму. Таким чином, наявність у науковця праць, опублікованих в рецензованих виданнях, свідчить про його певний рівень, навіть якщо ці видання з тих чи інших причин відсутні в міжнародних НБД.

Scopus і Web of Science індексують лише рецензовані видання (що мають ненульовий імпакт-індекс), тому така поправка не вплине на стандартний SCI. Але для національних НБД вона може бути суттєвою, оскільки знизить показники для науковців, що не мають належного фахового рівня.

Як кількісну міру рівня рецензування можна (в найпростішому випадку) обрати відношення кількості публікацій в рецензованих виданнях до загальної їх кількості, виражене в процентах. Тоді повний наукометричний покажчик міститиме три члена: SCI за міжнародними НБД, SCI за національними НБД та рівень рецензування. Як один з можливих варіантів, можемо запропонувати конструкцію X.Y.Z, де X, Y, Z – відповідні складові повного покажчика. Наприклад, 028.037.64 означає, що SCI за даними Scopus становить 28, SCI за даними національних НБД становить 37, а рівень рецензованості становить 64 %. Така конструкція містить всю важливу інформацію щодо оцінки наукової діяльності за різними доступними методиками. Головна перевага такого покажчика полягає в тому, що він не спотворює дані, визнані міжнародною спільнотою.

Висновки.

Ми бачимо, що технологія створення, наповнення та експлуатація наукометричних баз даних породжує специфічні проблеми, які не можуть бути вирішені лише вдосконаленням технічних засобів.

Головною, на наш погляд, є принципова неповнота наукометричних баз даних при наявних наукометричних методиках. Наслідком є те, що за певних умов виникає невідповідність між формальними наукометричними параметрами і реальним науковим рівнем як окремих науковців, так і наукових організацій.

В роботі як один із можливих напрямків вирішення зазначеної проблеми пропонується узагальнена кількісна міра наукової ефективності, яка не потребує нових методик отримання додаткових даних, але разом з тим нівелює головні недоліки стандартних наукометричних оцінок.

Ця міра може бути побудована шляхом розширення наукометричних баз даних за рахунок індексації додаткових джерел в межах окремої країни з використанням комплексних наукометричних методик, а також врахування рецензування наукових праць. Запропонований параметр містить три складові: стандартні наукометричні оцінки, побудовані за міжнародними та національними наукометричними базами даних, а також параметром, який компенсує певні суперечності між ними .

Отримані висновки можуть бути використані й для інших методик, яких ми не будемо торкатись.

Використана література

1. Налимов В.В., Мульченко З.М. Наукометрия. Изучение науки как информационного процесса. Москва: Наука, 1969. 192 с.

2. Елин А.Л., Шапошников Ю.Ю. Заметки к вопросу об эффективности использования различных наукометрических показателей и критериев эффективности научных исследований *Научная периодика: проблемы и решения*. 2013. Т. 3. № 3. С. 4-12. URL: https://bgscience.ru/lib/101793

3. Garfield E. Citation Indexes in Sociological and Historical Research. American documentation. 1963. V. 14. P. 290.

4. Кара-Мурза С. Цитирование в науке и подходы к оценке научного вклада. *Вестник АН СССР*. 1981. № 5. С. 68-75. URL: http://www.prometeus.nsc.ru/science/citation/ karmurza.ssi

5. Hirsch, J.E. (15 November 2005). ‘An index to quantify an individual's scientific research output’. PNAS 102 (46): 16569–16572.

6. Що таке індекс наукового цитування та його завдання / Науково-дослідний інститут правового забезпечення інноваційного розвитку НАНПрУ. URL: http://ndipzir.org. ua/archives/4172

7. Garfield E. To cite or not to cite: a note of annoyance. Current Contents. 1977. V.9. № 35. P. 6.

8. Garfield E. Is citation analysis a legitimate evaluation tool? Scientometrics. 1979. V.1. № 4. P. 359-376.

9. Індекс цитувань. URL: https://uk.wikipedia.org/wiki/%D0%86% D0%BD%D0%B4%D0%B5%D0%BA%D1%81_%D1%86%D0%B8%D1%82%D1%83%D0%B2%D0%B0%D0%BD%D1%8C

10. Scopus. URL: https://www.elsevier.com/solutions/scopus

11. Web of Science. URL: https://clarivate.com/products/web-of-science

12. Google Scholar. URL: https://scholar.google.com.ua

13. SciVerse. URL: https://www.sciverse.com

14. Scopus Content Coverage Guide. URL: http://www.webcitation.org/6Hktb4idO

15. Азбель М. Иерусалимские размышления. *“Природа”*. 1991. № 10. URL: http://www.bioacoustica.org/publ/papers/Azbel_1991.pdf

16. Бібліометрика української науки. URL: http://nbuviap.gov.ua/bpnu

17. Український індекс наукового цитування. URL: http://kpi.ua/uincit

18. Все украинские журналы в Scopus и Web of Science. URL: https://open science.in.ua/ua-journals

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

Інформаційна і національна безпека

УДК 340+35.078.3

ДОВГАНЬ О.Д., *доктор юридичних наук, старший науковий співробітник,*
НДІІП НАПрН України
ТКАЧУК Т.Ю., *кандидат юридичних наук, доцент,*
ННІ інформаційної безпеки НА СБ України

НАУКОВА РЕФЛЕКСІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: ВІД ПОЗИТИВІЗМУ ДО МЕТАФІЗИКИ ПРАВА

Анотація. *У статті досліджуються історичні засади становлення сучасного розуміння інформаційної безпеки. На основі використання філософських методів досліджено особливості змісту інформаційної безпеки, критично проаналізовано сутнісні її характеристики. Визначені основні пріоритети розвитку інформаційного суспільства на сучасному етапі.*

Ключові слова: *інформаційна безпека України, забезпечення інформаційної безпеки, національна безпека, система, стан, процес, загроза.*

Summary. *The article investigates the historical principles of formation of modern understanding of information security. On the basis of the use of philosophical methods, the features of the content of information security have been investigated, its essential characteristics are critically analyzed. The main priorities of the information society development at the present stage are defined.*

Keywords: *information security, information security ensuring, national security, state, process, threat.*

Аннотация. *В статье исследуются исторические основы становления современного понимания информационной безопасности. На основе использования философских методов исследованы особенности содержания информационной безопасности, критически проанализированы сущностные ее характеристики. Определены основные приоритеты развития информационного общества на современном этапе.*

Ключевые слова: *информационная безопасность, обеспечение информационной безопасности, национальная безопасность, система, состояние, процесс, 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 інформаційної безпеки.

А прецінь, їх погляди є найбільш показовими як у своїй протилежності, так і в єдності, що може стати тим перспективним аспектом осмислення сутності інформаційної безпеки України, 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. Окрім того, філософський аналіз даної проблеми потрібен для вибору перспективної методології дослідження питань інформаційної безпеки України.

Результати аналізу наукових публікацій. Проблематика інформаційної безпеки та її забезпечення у різних аспектах висвітлювались у наукових працях Плутарха, Сенеки, Платона, Макіавеллі, Гроція, а також інших вітчизняних та зарубіжних дослідників. Водночас, слід констатувати, що в сучасній доктрині інформаційного права залишено поза увагою дослідження тих філософсько-методологічних платформ на яких має базуватися інформаційне право у перспективі. На практиці це приводить не лише до активізації наукової дискусії, але й до неадекватності розуміння змісту тих або інших положень, висновків і рекомендацій, що стосуються сфери інформаційного права.

Метою статті є визначення перспектив розвитку метафізичного методу дослідження в інформаційному праві, а також з'ясування місця і ролі діалектики та юридичного позитивізму у дослідженнях інформаційного права.

Виклад основного матеріалу. Дослідження будь-яких явищ, в тому числі й правових, неминуче зачіпають філософську методологію, яка в правничій науці слугує своєрідним евристичним орієнтиром у розробці абстрактних правових конструкцій та понять, у розробці критеріїв оцінки суспільних відносин на предмет законності, а також безпосередньо бере участь у формуванні предмету дослідження. Можна припустити, що саме через філософське трактування суспільні відносини набувають ознак правовідносин. Право теж є метафізичною категорією, адже саме по собі воно нічого не регулює, це роблять конкретні люди, свідомо обмеживши свої дії правом.

Перша половина 21 століття яскраво продемонструвала чіткий перехід на новий виток дослідження права: на зміну антропології права, характерним відображенням якого є правовий позитивізм, приходить метафізика права, особливістю якої є наявність ірраціонального у праві. З приводу зазначеного відомий теоретик права І. Ісаєв розглядаючи поняття метафізики пише, що "сучасний" правовий позитивізм і нормативізм виключили це поняття з наукового обігу. Але разом з цим право втратило багато своїх особливо тонких і глибоких рис, а "буква вбила дух". Правова реальність набагато глибша і різноманітніша, ніж набір кодифікованих норм" [1, с. 3].

У продовженні цієї думки наведемо вислів римського юриста Павла: "Чинить проти закону той, хто робить заборонене законом; чинить в обхід закону той, хто, зберігаючи слова закону, обходить його сенс" [2].

"Дух закону", перш за все, пов'язаний з сутністю права, а також з його осмисленням і наділенням норми права змістом, сенсом. Можна сказати, що людина порушуючи закон не розуміє його суті і не прагне до її пошуку. Саме зміст і його пошук є ключовим у понятті "дух" права.

Ще однією особливістю метафізики права є людиноцентризм. Право має відійти від забезпечення інтересів тих, хто його створює і цілковито бути відданим служінню людині. Безперечно тільки людина, її природні права мають бути центром гуманізації та оптимізації правової системи. Принцип *"Salus populi suprema lex est"*[1] має стати чітким орієнтиром сучасної правової системи.

Серед системи природних прав особливе місце займає право на інформацію. Спірність включення даного права до природних є сумнівною. Адже виходячи із загальноприйнятих особливостей природного права людини (надані людині від природи; носять природний і невідчужуваний характер; виступають у якості найвищої соціальної цінності; є безпосередньо діючим правом; знаходяться під захистом держави; відповідають міжнародним стандартам) право на інформацію цілком відповідає згаданим критерієм.

[1] Благо народу – вищий закон.

Розвиваючи дану думку, слід окремо підкреслити, що на основі права на інформацію відбувається осмислення права людиною як елемента формування безпечного середовища проживання. Це пояснюється тим, що при здійсненні будь-якої фізичної або інтелектуальної діяльності людина завжди стикається з інформацією: процесом її отримання, обробки, структурування, та навіть прийняття будь-якого рішення потребує інформаційної підтримки. Таким чином будь-яка діяльність людини є процесом пізнання. У цьому процесі пізнання людина, багато в чому, через інстинкт самозбереження намагається всі явища або об'єкти, які їй невідомі, зрозуміти і пояснити в своїй свідомості на основі отриманої інформації. Фактично, людина з'ясовує їх ступінь небезпеки для себе та суспільства в цілому. Цим людина формує безпечне середовище для своєї життєдіяльності, що в загальному, можна назвати відображенням її біологічної природи. Таким чином "народжується" категорія "інформаційна безпека людини, суспільства, держави". Окреслені процеси і є відображенням метафізичного у праві.

Отже, можна з упевненістю стверджувати, що з правом на інформацію тісно пов'язана інша системоутворююча категорія – "інформаційна безпека". Більше того, право на інформацію виступає певним індикатором її стану. Адже це найочевидніший елемент у порівнянні з іншими (інформаційна безпека суспільства, інформаційна безпека держави). Більше того, при порушенні права на інформацію людини, тобто зазіхання на інформаційну безпеку людини, інформаційна безпека суспільства і держави однозначно будуть піддаватися негативному впливу як від загроз іззовні, так і внутрішніх загроз.

Хоча, у Конституції України й закріплено, що забезпечення інформаційної безпеки – це одна з найважливіших функцій держави, справа всього народу (ст. 17), в інших правових актах або звужено зміст інформаційної безпеки (*Доктрина інформаційної безпеки України*), чи взагалі не розкривається, що потребує законодавчого врегулювання.

Сучасні наукові підходи до концепції інформаційної безпеки ґрунтуються на багатій філософській базі, розвиток якої починається ще з давніх часів. Мислителі різних епох завжди шукали причини і джерела небезпек, прагнули домогтися стійкого миру, безпеки та процвітання, в ході чого й змінювалися погляди на інформацію. Питання безпеки особи, суспільства, держави та отримання достовірної інформації про це хвилювали філософів Стародавнього світу. Щоправда, вказана проблема розглядалася переважно в контексті війни й миру [3, с. 40]. Водночас слід підкреслити, що для філософської культури Стародавнього світу був характерний синкретизм, тобто для тогочасної наукової думки не існувало розподілу між сферами духовної діяльності людини.

Коли йдеться про інформаційно-комунікаційні технології, передовсім маються на увазі засоби зв'язку чи, швидше, канали зв'язку. З найдавніших часів зв'язок асоціювався з магією. Одним з різновидів магії був звук. Людський голос (звук, який видається людиною) вважався магічним за своєю природою. У книзі Буття Адам виконував магічну за своєю суттю дію, даючи найменння рослинам і тваринам. Таким чином він підтверджував дану йому Богом могутність, а проголошення назв стало справжньою демонстрацією магічних можливостей. Самі імена теж наділялися магічною силою. Так, у древньому іудаїзмі ім'я Бога само по собі було ототожненням могутності, а промовляти його міг лише первосвященик раз на рік, перебуваючи наодинці у найсвятішій частині Храму. У багатьох культурах особи, які проходили певні ритуали посвячення, отримували нові й часто втаємничені імена. За давньою ірландською легендою поет, котрий мав магічну здатність управляти мовою, міг прокляти будь-яку людину, давши їй ім'я із "вплетеним" у нього прокляттям.

Якщо зв'язок вважався за своєю природою магічним, то аналогічним було ставлення й до процесу підтримки цього зв'язку. До прикладу, давньоєгипетський бог Тот "опікувався" як магією й мудрістю, так і писемністю, причому різниці між цими поняттями практично не існувало. У древньоєврейському алфавіті, а пізніше й у Кабалі літери і слова самі по собі вважалися носіями магічної сили. Так, слова *"вимовляти"* та *"читати заклинання"* були синонімами. У багатьох стародавніх культурах ті, хто мав доступ до цієї особливої магії – до загадкових таємниць знаків і звуків, які забезпечували й оберігали зв'язок, – вважалися хранителями магії.

Що менш доступними були засоби зв'язку, перетворюючись на прерогативу посвячених, то більше вони асоціювалися з таємницею та магією. Відомо, що німецький гуманіст, лікар, алхімік, натурфілософ, окультист, астролог і знаний адвокат Агріппа Неттесгаймський листувався з ученими інших країн, а пізніше зміцнював свій імідж мага, видаючи отриману від них інформацію за повідомлення духів.

Абсолютно не принципово, що наш розум сьогодні звик сприймати ці речі як продукти технології, а не магії. До того як картезіанське мислення призвело до фрагментації знання, магія і технології були єдині. Нині вони залишаються нероздільними лишень у метафоричному сенсі. Проте, незалежно від термінології, багато хто й донині продовжує говорити про "мистецтво створювати події". Від Агріппи до нас пройшло дуже багато часу. Змінися й технології. Ми живемо в епоху цифрових технологій і вже не уявляємо нашого буття без Інтернету, електронної пошти та інших плодів технологічного прогресу. Проте і сьогодні, як сказав більше двох століть тому Натан Ротшильд, *"хто володіє інформацією, той володіє світом"*[2], залишається актуальним. Тобто володіння інформацією залишається певним магічним дійством, здатним впливати на маси, результати парламентських чи президентських виборів, ставати збудником революцій, війн і т.д. І якщо цей світ являє собою найбільш яскраву на сьогодні демонстрацію магічної сили, то він також є потужною потенційною силою для маніпуляцій свідомістю, а це і є своєрідною магією. Якщо ж відбуваються якісь впливи на поведінку людини чи груп людей, логічно постає й категорія "безпеки", котра в цьому разі матиме дуалістичну характеристику: безпека інформації як інструменту впливу та безпека від інформації, яка може вплинути. В обох випадках суб'єктний склад різний.

Історія інформаційної безпеки (хоча раніше її так не називали) сягає корінням сивої давнини. Приміром, ще цар Давид у своїй молитві промовляв: *"Ти погубиш тих, хто говорить брехню; кровожерним і підступним гребує Господь"* [4, с. 370]. Брехня в даному разі, як би ми сказали сьогодні, це – "дезінформація" чи "недостовірна інформація". Суб'єктів розповсюдження такої інформації Давид характеризує вельми суворо, що, вочевидь, означає тяжкість подібних діянь. Давньогрецький письменник, історик і філософ-моралість Плутарх згадує звичай, коли кожного, хто входив до сессітії, старший, показуючи на двері, попереджав: "Жодне слово з них не виходить" [4, с. 181]. Це свідчить про розуміння неабиякої важливості вміння зберігати секрети в таємниці, а також про те, що вже тоді існували прототипи сучасних секретоносіїв. Своєю чергою, давньоримський філософ, поет та державний діяч Сенека у праці "Едип-цар" застерігає від використання недостовірної інформації, говорячи устами свого героя, що виявлення

[2] Сказані вони були після того, як голуби, якими захоплювався Натан і його брат Якоб, першими принесли їм звістку про поразку Наполеона під Ватерлоо. Це дозволило братам-банкірам виграшно зіграти на Лондонській та Паризькій біржах і стати володарями більшої частки британської економіки. Хоч сказані ці слова були і Ротшильдами, але популярною ця фраза стала після того, як її повторив Вінстон Черчель.

довіри віроломному – надати йому можливість шкодити [5, с. 142]. А сентенцією "безпека є запобіганням шкоді" Платон фактично говорить про інформаційну розвідку [6, с. 415].

Ведучи мову про інформаційну безпеку держави, неможливо обійти увагою духовного натхненника інформаційних війн китайського військового стратега й філософа Сунь-Цзи (313-239 рр. до н. е.), який написав першу у цій сфері фундаментальну працю під назвою "Мистецтво війни", де, зокрема, говориться: *"Якщо прогресивний володар або мудрий генерал отримує перемогу над противниками кожного разу, коли вони переходять до дії, то це досягається завдяки попередній інформації. Так звана попередня інформація не може бути отриманою ні від духів, ані від божеств, ні за аналогією з попередніми подіями, ані шляхом розрахунків. Її необхідно отримати від людини, знайомою із ситуацією супротивника"* [7, с. 93]. В основі концепції Сунь-Цзи лежить теорія управління ворогом: *"його заманюють в пастки вигодою, позбавляють хоробрості, послаблюючи й виснажуючи перед атакою"* [7, с. 10].

Якісно новий етап формування елементів науково-філософських концепцій безпеки пов'язаний з епохою Відродження. У центрі уваги передових мислителів цього періоду стояла людина, її духовне життя (інформаційна сфера), її звільнення з-під церковного гніту й соціальної несправедливості. Осмислення умов безпечного гармонійного розвитку особистості призвела гуманістів до постановки питання про усунення з життя людей найбільшого зла – війни. Народженню ідеї вічного миру сприяло, безперечно, перетворення війни на далі більшу загрозу для народів Європи. Удосконалення зброї, створення численних армій і воєнних коаліцій, багаторічні війни, що продовжували роздирати європейські країни у ще ширших масштабах, аніж раніше, змусили мислителів епохи Відродження задуматися над проблемою безпечних міждержавних стосунків і шукати шляхи їх нормалізації, зокрема, шляхом обміну інформацією стосовно безпекових питань.

У XVI столітті італійський мислитель Нікколо Макіавеллі сформулював інформаційно-психологічну концепцію державної влади, де виклав основні принципи інформаційного протиборства в політичній сфері [8]. Крім того, історія багата прикладами проведення потужних інформаційно-пропагандистських акцій, класичних варіантів глобальної дезінформації народу, які відіграли свою фатальну роль.

На початку XVII ст. здійснюються спроби юридичного впорядкування міждержавних відносин. Одним із засновників теорії природного права й міжнародно-правової науки став голландський мислитель Гроцій Гуго де Гроот. Його трактат "Про право війни і миру", присвячений передусім проблемам міжнародного права, містить основні положення цієї галузі: договори між державами, які дотримуватимуться через природний закон, мають замінити владу Папи Римського; слід заборонити несправедливі війни, що порушують будь-чиє право; воюючі сторони зобов'язані утримуватися від винищення ворожої власності й жорстокості щодо цивільного населення. Г. Гроцій пропонував також заснувати орган для розв'язування суперечок між державами, який би мав ефективні (у тому числі інформаційні) засоби примусу [9, с. 145-147]. Заслуга основоположника науки міжнародного права полягала й у тому, що він, розуміючи складність усунення збройного насильства, розвивав ідеї його гуманізації, обміну інформацією та регулювання відносин між державами на користь миру й безпеки.

У XVII ст., коли завершувалося становлення більшості національних держав Європи, окреслився етап обґрунтування ідеї "вічного миру". На відміну від "християнського миру", що містить у собі релігійну нетерпимість і апологетику, а то й

заклик до боротьби з невірними, більшість проектів "вічного миру" відображали успіхи емпіричної філософії й раціоналістичний підхід. У таких проектах часто фігурував "державний інтерес" у створенні міцного миру й забезпеченні стійкої безпеки як реальної передумови процвітання молодих держав. Ідеться про "Політичний заповіт" А.-Ж. Рішельє, "Досліди" Ф. Бекона та ін.

Наукове ж обґрунтування проблеми національної безпеки взагалі, й інформаційних її аспектів зокрема, в сучасному розумінні й певні напрямки її вирішення містяться у працях Томаса Гоббса та Іммануїла Канта. Як слушно зазначає український дослідник проблем безпеки О. Дзьобань, погляди Гоббса й Канта на сутність досліджуваної проблеми є найбільш характерними в даному контексті [10, с. 41]. Розуміючи як природний стан беззаконня й наявності у кожного права на все, Кант та Гоббс приходять до необхідності встановлення громадянського устрою, за якого забезпечувалася би безпека індивіда. Попри принципові розбіжності у поглядах філософів на процесуальні аспекти досягнення безпечного стану, їхні теорії збігаються у тому, що споконвічно притаманна індивідам повна свобода обмежується ними (теоріями) заради безпеки в усіх аспектах її розуміння, але безпека дає змогу цю свободу реалізувати.

Фундаментальні ідеї гоббсівського й кантівського вчень про безпечне існування особи, суспільства й держави, способи забезпечення миру й безпеки набувають особливої актуальності в сучасних умовах інтенсивного розвитку загальноєвропейського й світового процесу в напрямку визнання й поступового ствердження ідей панування права, принципів свободи й рівності. Міркування цих мислителів стосовно проблем безпеки продовжують відігравати величезну роль в усвідомленні того, де ми знаходимося й куди маємо рухатися, аби вийти на правильний шлях до майбутнього безпечного існування. В сучасних умовах пошуку оптимальних варіантів розв'язання проблеми забезпечення безпеки індивідів, суспільств, держав та їх союзів органічне поєднання раціональних зерен обох наведених теорій, безумовно, сприятиме віднайденню того оптимального стану й способу забезпечення інформаційної безпеки, який буде прийнятним для різних суспільних утворень у багатополюсному сучасному світі.

Ідеї безпеки у період раннього Просвітництва знайшли своє відображення у філософській і політичній творчості Джона Локка. Розробкою філософських питань безпеки через релігійно-етичне розуміння проблеми миру займалися в епоху Просвітництва Ф. Вольтер, Д. Дідро, гоббсівську позицію підтримував Ж.-Ж. Руссо; в період німецької класичної філософії Й. Фіхте та Й. Гердер, котрі під різними кутами зору розглядали ідею забезпечення безпеки через обґрунтування державного суверенітету.

Багато цікавих ідей щодо вирішення безпекових проблем висунули соціалісти-утопісти Клод Анрі де Рувруа Сен-Сімон, Шарль Фур'є і Роберт Оуен. Так, Сен-Сімон – французький мислитель, соціолог, один із засновників утопічного соціалізму, запропонував ідею своєрідної колективної безпеки народів. Він уважав, що його філософська система, котру він назвав "новим християнством", "оновленою релігією", є інформаційним підґрунтям, покликаним "створити для всіх народів стан вічного миру й безпеки, об'єднуючи їх проти тієї нації, яка побажала би досягти свого власного блага за рахунок загального блага всього людства. Таке досягнення здійснюється шляхом об'єднання їх (народів) проти всякого уряду, який пройнятий антихристиянським духом до такої міри, щоб загальнонаціональні інтереси принести в жертву приватним інтересам правителів" [11, с. 411]. Очевидно, що така ідея, як на той час, так і сьогодні, не є обґрунтованою і для наукового аналізу серйозно сприйматися не може.

Валлійський філософ, педагог та соціаліст-утопіст Роберт Оуен уважав, що початок якісно нового безпечного стану – вселюдської гармонії – може покласти лише належним чином організоване виховання людей на підставі доцільного застосування інформаційних аспектів виховного процесу Він підкреслював, що тільки звільнення народів від приватновласницького ярма й об'єднання їх в один союз покладе край насильству й уможливить забезпечення безпеки [12, с. 375]. Окремі елементи теорії Р. Оуена (які стосуються союзницьких лозунгів) спостерігаються сьогодні в умовах глобалізаційних тенденцій, однак поєднати в єдиний науковий підхід його розуміння принципів виховання і принципів об'єднання людей вельми проблематично, а тому можливості застосування даної точки зору для сучасного розуміння проблем інформаційної безпеки достатньо обмежені.

Французький філософ Анрі Бергсон, поєднуючи інформаційну безпеку з розумінням закритого й відкритого суспільств, зазначав, що насильство й війни є неминучим наслідком закритих суспільств і, отже, сумною необхідністю епохи. Єдину можливість подолання проявів насильства, несправедливості, роз'єднаності людей і досягнення безпечного стану існування людства він убачав у пропаганді "духу простоти", сповіщеного християнськими містиками, принципів аскетизму, у відмові від "штучних потреб", спричинених переважанням розвитку в останні століття "тіла" людства, а не його "душі" [13, с. 269].

Англійський філософ, логік і мораліст Бертран Рассел у своїх численних творах попереджав людство, що настав вирішальний момент історії, коли воно мусить зробити вибір: або загинути внаслідок війни (оскільки сучасна зброя вражає обидві сторони), або цю небезпеку перемогти. Розум повинен узяти гору над безглуздям, і особливе місце у даному процесі має належати формуванню та спрямуванню необхідних інформаційних потоків (впливів) [14, с. 77].

Мислителі різних епох засуджували насильство, пристрасно мріяли про вічний мир і безпеку, пропонували різні моделі здійснення своїх задумів. Одні з них звертали увагу насамперед на інформаційно-етичний бік проблеми (Августин Блаженний, І. Кант, Р. Оуен, А. Бергсон, А. Швейцер). Вони вважали, що агресія, війна є породженням аморальності, що безпечного стану можливо досягти тільки шляхом морального перевиховання людей у дусі взаєморозуміння, терпимості до різних віросповідань, усунення націоналістичних пережитків, виховання людей за принципом "усі люди – брати". Інші вбачали головну перешкоду для досягнення безпечного суспільного стану в господарській руїні, в порушенні нормального функціонування всієї економічної та інформаційної структур (Ціцерон), у колізії природного й громадянського станів особистості (Т. Гоббс, Дж. Локк). У зв'язку з цим вони намагалися схилити людство до миру й безпеки, малюючи картини загального процвітання в суспільстві без воєн, у якому пріоритет надаватиметься розвитку науки, техніки, мистецтва, літератури, інформації, а не вдосконаленню засобів знищення. Вони вважали, що міждержавну безпеку можна встановити завдяки розумній політиці освіченого правителя. Треті розробляли правові аспекти безпеки, досягти якої вони пропонували шляхом угоди між урядами, створенням регіональних або всесвітніх федерацій держав (Г. Гроцій, Сен-Сімон, К. Ясперс, А. Тойнбі). Четверті переконували, що коріння небезпек має соціальний характер, що усунути їх можна, лише змінивши структуру суспільства (Еразм Роттердамський, С. Франк).

Інформаційна безпека держави це завжди сутнісне діалектичне поняття, оскільки безпека може існувати лише в контексті небезпеки, постійних загроз, постійного процесу виявлення цих загроз, їх локалізації, зменшення негативного впливу, прогнозу

на майбутнє. А тому, правильним убачається твердження А. Нашинець-Наумової, що інформаційна безпека здатна до розвитку і саморозвитку, тому будь-яке наукове знання про неї набуває актуального значення. Інформаційну безпеку України можна інтерпретувати як сукупність життєво важливих умов функціонування суб'єктів (*людини, суспільства, держави*) в інформаційній сфері та суб'єктивних (*правових, політичних, інформаційних, наукових, оперативно-розшукових*) можливостей їх усвідомлення й контролю [15, с. 4, 10].

Попри таке її основне й найбільш поширене розуміння, "інформаційна безпека" (зокрема, і як об'єкт права) є поняттям неоднозначним. На це є дві основні причини.

По-перше, фундаментальні закономірності розвитку матерії залишаються досі недостатньо дослідженими, що спонукає фахівців послуговуватися терміном "інформація" для опису маловивчених і часто непорівнянних явищ, пов'язаних з об'єктами матеріального світу, зокрема, із системами живої та неживої природи.

По-друге, величезні потенційні можливості кібернетики, яка створила передумови для виникнення уявлень про самоорганізовані системи як єдину форму існування матерії, наразі увійшли в суперечність з обмеженими операційними можливостями поняття "інформація" К. Шеннона [16], за допомогою якого досі намагаються розкрити гносеологію, генезис та онтологію цих систем. По суті, ця суперечність насправді була закладена ще Н. Вінером [17], котрий у своїх працях терміном "інформація" позначав "робоче тіло", за допомогою якого забезпечується управління. Одначе цей термін позначає дещо інші явища. Ми чітко бачимо, що головні підходи та концепції до розуміння основних сутностей інформаційної безпеки проходять етап від діалектичного пізнання до синергетичного їх розуміння.

У рамках позитивізму відбулося знецінення права до рівня інструкції з повсякденної діяльності, позбавленого будь-якого сенсу, пов'язаного з культурною, філософсько-релігійною, національною спадщиною людської цивілізації (метафізична реальність права). Сам Дух права втратив свій первісний лик. У рамках метафізики права відбувається його переосмислення, відродження та формування майбутніх шляхів розвитку. Особливо це актуалізується із розвитком таких інноваційних напрямів інформаційного права як IT-право, право роботів, правові межі штучного інтелекту тощо. Як бачимо, в наш час особливої динамічності набуває інша складова права, як елемента формування безпечного середовища проживання – реалізація творчого потенціалу, першочергово це створення якісно нових предметів матеріального світу і відповідно системи знань щодо управління ними та їх експлуатації, що теж є відповідним процесом пізнання. У цьому процесі інформація відіграє теж архіважливе значення. Допомагає віднайти людині сенс, суть, головне призначення створених чи створюваних предметів. На цьому етапі особливого значення, у рамках інформаційної безпеки, набуває здатність та вміння людини до критичного мислення, медіа грамотність, інформаційна культура та інше.

"Інформація несе у собі як творчу, так і руйнівну силу, але набагато більшою мірою, аніж це було раніше" [18, с. 33]. Отже, поряд з безпекою інформаційних технологій та інформаційних ресурсів не менш важливим, на наш погляд, є гуманітарний вимір інформаційної безпеки, тобто захист від інформації та інформаційна вразливість людини, суспільства, держави, цивілізації.

Нинішній етап світової історії характеризується переходом людства від індустріальної до інформаційної цивілізації, в основі розвитку якої покладено знання, засновані на інформації. Водночас суспільство, на думку українських дослідників,

“з великим запізненням починає осмислювати політичні, економічні, соціальні, військові, психологічні та інші наслідки глобальної інформатизації” [18, с. 35].

Висновки.

Сакральний зміст поняття “інформація” не розкрито до цих пір. Загальноприйнята теорія Шенона вирізняється формальним, чи навіть абстрактним трактуванням інформаційних зв’язків. Проте сама цінність інформації для споживача не береться до уваги. Напевне тому сам Шенон свою теорію назвав “математична теорія зв’язку”. За Шеноном повідомлення – певні кодові пересилання передавача, а не сам зміст повідомлення. Наразі людство у своєму розвитку перейшло у *фазу змістовного аналізу інформації*. Це пов’язано, першочергово, із збільшенням обсягів інформації, розвитком ІКТ, Інтернету-речей, ІТ-права тощо. Відповідно, особливого значення набуває критичне мислення, критичний аналіз та екологія інформації. *У недалекому майбутньому поняттям інформації буде охоплюватися тільки цінна інформація, яка енергетично збагачує та дає можливість реалізувати мету. Все інше буде на кшталт інформаційного шуму та марних (пустих) даних.*

Епоха індустріальної цивілізації, основою якої була машинна техніка, відходить у минуле. Їй на зміну прийшла інформаційна ера, яка заснована на знаннях. Один з висновків Пола Ромера, який отримав Нобелівську премію у 2018 році у галузі економіки за розробку власної економічної моделі, містить твердження, що економіка, яка володіє ресурсами людського капіталу та розвиненою наукою, в довгостроковій перспективі має кращі шанси на зростання, ніж економіка, позбавлена цих переваг. Якщо традиційна економіка розглядає тільки два фактори виробництва – капітал і працю, то модель Ромера додає третій – технологію, як результат людського інтелекту. По-суті, П. Ромер змінив макроекономічну модель, яка була до нього.

Відповідно, вельми вагомою складовою інформаційної безпеки виступає *соціальна безпека* суспільства. Ця складова інформаційної безпеки передбачає захист у соціальній сфері інтересів народу і країни, формування громадських структур і соціальних відносин, системи життєзабезпечення, способу життя, що відповідає вимогам прогресу сучасного суспільства та гідного рівня життя людей.

Можливості сьогоднішніх інформаційних технологій значно підвищили ефективність впливу інформаційних засобів на психіку і свідомість людей, відкрили нові методи і прийомами прихованого маніпулювання. Людина – головна мета інформаційного механізму управління. Загроза дегуманізації набула настільки реальних обрисів, що у структурі сучасних цінностей найголовнішим благом стало виступати саме життя людини. Державно-правова захищеність людини від фізичних посягань зазвичай вища, ніж від зазіхань на психіку людей. Правова сфера часто відстає від процесів суспільного розвитку, а в духовній сфері це відставання в рівні захищеності стало просто катастрофічним. Відтак, першорядного значення набуває правова захищеність свідомості людей.

Спотворені методи використання інформаційних технологій призвели до деформаційних змін соціальної сфери. Це відбилося передовсім у спонуканні соціального розшарування суспільства за допомогою розподілу інформаційних послуг і благ, диссолюції інститутів, спрямованих на розвиток особистості, підбурюванні до розколу на підставі етнічної, національної, ідеологічної, релігійної, мовної ознак. У соціальній сфері українського суспільства наслідки зазначеної інформаційної агресії суттєво проявляються вже тривалий час.

У контексті даного дискурсу слід окремо звернути увагу на засоби масової інформації, які багато в чому є чи не найважливішим елементом інформаційного

суспільства. У теперішній час засоби масової інформації по суті монополізували процес задоволення інформаційних потреб населення у світі, країні, регіоні, на підставі чого спроможні нав'язувати ідеологічні погляди й настанови. Тому критично назріла нагальна потреба порушувати питання про ступінь довіри до інформації, яка транслюється ЗМІ, та її якість, позаяк засоби масової інформації здатні сьогодні виступити в ролі надпотужної сили, спрямованої як на стабілізацію суспільства, так і на спричинення соціального вибуху. Не зайвим буде додати, що відповідні заходи стосовно ЗМІ мають здійснюватися виключно у правовому полі. Таким чином, без належного правового забезпечення інформаційної безпеки неможливо досягти бажаного рівня соціальної безпеки.

Більше того, сьогодні активно дискутується питання про так звану екологію інформації. Показовою з цього приводу є праця Фелікса Сталдера, яка так і називається – "Екологія інформації" [19]. На підставі свого дослідження вчений резюмує, що медіа створюють інтегроване середовище (environment), основу якого становлять потоки інформації. Дедалі частіше в діяльності людини це середовище стає головним. Екологія інформації прагне зрозуміти його властивості, щоб використовувати потенціал цього середовища, уникати небезпек і позитивно впливати на його розвиток.

У цьому контексті ми підтримуємо Р. Проданюка, який зазначає, що інформаційна безпека може розглядатись як одна із соціальних інституцій контролю за підтриманням інформаційної рівноваги, функція якої полягає в підтриманні екологічності інформаційного простору [20, с. 87].

Розвиток інформаційних технологій на початку XXI століття визначив загальні тенденції поступу людства та окреслив характерні проблеми даної епохи, серед яких:

1. Формування нового планетарного простору, в основі якого інформаційні й телекомунікаційні технології забезпечують ефективну взаємодію між людьми. Основними характеристиками таких процесів є безмежність, доступність, гіперпов'язаність, "стирання" територіальних кордонів, рух у масштабі часу, розвиток Інтернету речей тощо. Як наслідок, відбувається становлення нового інформаційного суспільства.

2. Усі без винятку суспільні процеси (політичні, соціальні, економічні) залежать від використання інформаційних технологій, оскільки вони мають вирішальне значення у формуванні існуючої реальності й мають неабиякий вплив на її розвиток.

3. Недостатня увага з боку як міжнародних інституцій, так і національних урядів, до проблем правового забезпечення інформаційної безпеки стали причиною виникнення та надшвидкого поширення понять "інформаційна зброя", "інформаційний тероризм" та "інформаційна війна", а також деструктивних впливів від позначуваних цими термінами явищ. Значне применшення завдань інформаційної безпеки стало причиною непрогнозованих економічних, соціальних, екологічних, політичних та інших потрясінь у системі безпеки. Унаслідок цього вирішення питань інформаційної безпеки із значним запізненням вийшло на перший план в усіх сферах суспільного життя і державної діяльності, як на національному, так і на міжнародному рівнях.

Використана література

1. Исаев И.А. Теневая сторона закона. Иррациональное в праве: монография (науч. изд.). Москва: Проспект, 2013. – 364 с.

2. Дигесты Юстиниана. URL: http://www.vostlit.info/Texts/Dokumenty/Byzanz/VI/520-540/Digestae_Just/index.htm

3. Псалтирь. Харьков: Фолио, 2013. 574 с.

4. Плутарх Сравнительные жизнеописания / пер. с древнегреч. В. Алексеева. Харьков: Фолио, 2013. 348 с.

5. Сенека Л.А. Трагедии / пер. с лат. С. Ошерова, коммент. Е. Рабинович. Москва: Искусство, 1991. 494 с.

6. Платон. Диалоги / вступ. ст., коммент. А.Ф. Лосева / пер. с древнегреч. М.С. Соловьева. Москва: Зксмо, 2007. Кн. 1. 1231 с.

7. Сунь-цзы. Искусство войны: Древнейший в мире трактат о войне / пер. с кит., коммент., примеч. Л. Джайлса. 2-е изд. Ростов-на-Дону: Феникс, 2003. 283 с.

8. Николо Макиавелли. Государь. Москва: Олма Медиа Групп, 2011. 512 с.

9. Гроций Г. О праве войны и мира. Три книги, в которых обьясняются государственное право и право народов, а также принципы публичного права / пер. с лат. А.Л. Саккетти. Москва: Гос. изд-во юрид. лит-ры, 1957. 868 с.

10. Дзьобань О.П. Національна безпека України: концептуальні засади та світоглядний сенс: монографія. – Харків: Майдан, 2007. 284 с.

11. Сен-Симон А. Избранные сочинения / пер. с франц. под ред. и с коммент. Л.С. Цетлина, вступ. ст. В.П. Волгина. Москва-Ленинград: АН СССР, 1948. Т. 1. 468с.

12. Оуен Р. Організаційна поведінка в освіті: Керівництво учбовими закладами та шкільна реформа / пер. з англ. О.В. Христенко. Харьков: Каравела, 2003. 488 с.

13. Бергсон А. Творческая зволюция. Материя и память. Минск: Харвест, 1999. 1407 с.

14. Рассел Б.А. Человеческое познание, его сфера и границьі / пер. с англ. Н.В. Воробьева. Киев: Ника-Центр; Москва: Институт общегуманитарных исследований, 2001. 560 с.

15. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім "Гельветика", 2017. 168 с.

16. Шеннон К. Работы по теории информации и кибернетике. Москва: ИЛ, 1963. 830 с.

17. Норберт Винер. Кибернетика или управление и связь в животном и машине. Москва: Советское радио, 1968. 325 с.

18. Канигін Ю.М., Кушерець В.І. Біблія та майбутнє науки: орієнтири сучасних знань. Київ: Т-во "Знання України", 2009. 163 с.

19. Felix Stalder Information Ecology A position paper (version 1.0) McLuhan Program in Culture and Technology, FIS, UofT, 1997. URL: http://felix.openflows.com/html/infoeco.html

20. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. *Грані* (науково-теоретичний альманах). 2018. Т. 21. № 4. С. 84-90

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

УДК 340.111+340.134 (477)+342.51(477)

ДОРОНІН І.М., *кандидат юридичних наук, доцент,*
завідувач наукової лабораторії НДІІП НАПрН України

ОБОРОННІ "БІЛІ КНИГИ": ПРАВОВІ АСПЕКТИ ІНФОРМУВАННЯ СУСПІЛЬСТВА ПРО ДІЯЛЬНІСТЬ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ У КОНТЕКСТІ ГРОМАДСЬКОГО КОНТРОЛЮ

Анотація. *У статті досліджено правові аспекти інформування суспільства про діяльність сектору безпеки і оборони шляхом періодичного видання узагальнюючих документів ("Білі книги"). Проаналізовано правові підстави та практику, що склалась в діяльності державних органів. Визначено проблемне коло правового регулювання та окреслено шляхи вдосконалення інформування громадськості.*

Ключові слова: *національна безпека, оборона, сектор безпеки і оборони, інформування, громадський контроль, Білі книги.*

Summary. *This paper examines legal aspects of public information in the field of national security and defense by periodic issuing of summarizing papers ("White papers", "White books"). Legislation and practices of state authorities was also reviewed. Problem areas in current legislation are identified. Author proposed some ways for overcoming existing gaps and other improvements.*

Keywords*: national security, defense, public information, civil control, White papers.*

Аннотация. *В статье исследованы правовые аспекты информирования общества относительно деятельности субъектов сектора безопасности и обороны путем периодического издания обобщающих документов ("Белые книги"). Проанализированы правовые основания и сложившаяся практика государственных органов. Определено проблемное поле правового регулирование и намечены пути усовершенствования информирования общественности.*

Ключевые слова*: национальная безопасность, оборона, сектор безопасности и обороны, информирование, общественный контроль, Белые книги.*

Постановка проблеми. Оновлення вітчизняного законодавства у сфері національної безпеки зумовило і зміни підходів у питанні впровадження цивільного (громадського) контролю за діяльністю державних органів, що забезпечують національну безпеку і оборону. Уточнення існуючих підходів далеко не повною мірою зумовило належну правову регламентацію форм і методів здійснення зазначених видів контролю, насамперед щодо періодичного видання узагальнюючих інформативних документів, які мають найменування "Білі книги", а також інших періодичних документів аналітичного характеру. Компетенція державних органів, розподіл завдань та уточнення обсягу повноважень потребують детального вивчення, аналізу практики та подальшого вдосконалення. Особливо це стосується форм і методів зазначеної діяльності.

Результати аналізу наукових публікацій. Проблематика забезпечення національної безпеки і оборони України та її правових основ постійно перебувала у полі зору науковців, водночас, питання здійснення громадського контролю у цій сфері, його форм, методів та обмежень залишаються мало дослідженими у літературі. На сьогодні окремі висновки та пропозиції з цього приводу містяться у численних роботах, що підготовлені під егідою Національного інституту стратегічних досліджень, а також окремих недержавних аналітичних центрів. Низка робіт, що готувалась фахівцями військових навчальних закладів та науково-дослідних установ (посилання на які будуть

зазначені в тексті цієї статті) містять певний аналіз змісту документів інформування громадськості в контексті дослідження особливостей військової політики. Водночас правові питання оприлюднення результатів діяльності суб'єктів сектору безпеки і оборони шляхом видання періодичних узагальнених видань (у тому числі Білих книг) на сьогодні залишаються поза увагою науковців.

Метою статті є проведення аналізу існуючої практики звітування перед громадськістю шляхом оприлюднення періодичного (не частіше ніж щороку) узагальнюючого документу (у вітчизняній практиці відомого як Біла книга), правових основ такої діяльності, дослідження підходів до формування та викладення змісту інформації у зазначеному документі. З урахуванням останніх законодавчих змін будуть вивчені підходи до оприлюднення інформації у системі громадського контролю, які пропонується запровадити.

Виклад основного матеріалу. Стаття 11 Закону України "Про основи національної безпеки України" від 19.06.03 р. з часу його прийняття містила загальні визначення щодо цивільного контролю за реалізацією заходів у сфері національної безпеки [1]. Такий контроль здійснювався відповідно Президентом України, Верховною Радою України, Кабінетом Міністрів України, Радою національної безпеки і оборони України в межах їх повноважень, визначених Конституцією і законами України.

Безпосередня регламентація недержавного (громадського, суспільного) контролю визначалась окремим Законом України "Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави" від 19.06.03 р. Одним із видів демократичного цивільного контролю законодавчо було визначено громадський контроль. Відповідно до вимог розділу IV цього Закону, громадський контроль здійснювався у вигляді участі громадян та засобів масової інформації у здійсненні контролю. З метою "систематичного інформування громадськості про діяльність Воєнної організації держави і правоохоронних органів, наявні проблеми в цій сфері та їх вирішення" відповідні органи державної влади та військового управління повинні були "періодично, за заздалегідь оприлюдненим розкладом", проводити прес-конференції, вміщувати на веб-сторінках Інтернету і оновлювати відповідні матеріали. З цією ж метою періодично (раз на рік) було впроваджено видання Білої книги про діяльність Збройних Сил України" [2].

Слід зазначити, що законодавча вимога про щорічне видання Білої книги про діяльність Збройних Сил України виконувалась. Зокрема, Міністерство оборони України щорічно видавало Білу книгу з питань реформування і діяльності Збройних Сил та оборонної політики. Як правило, відбувалось одночасне видання Білої книги українською та англійської мовами із широким залученням (на початковому етапі) фахівців провідних аналітичних центрів недержавного сектору безпеки та міжнародних організацій. До 2013 року включно було видано 9 щорічних Білих книг, з яких 3 присвячувались оборонній політиці, а 6 – організації Збройних Сил.

Започатковувалось видання "Білою книгою 2005". Воно було присвячене проблемам реформування Збройних Сил України з урахуванням поточного їх стану, перспектив та основних напрямів для подальшого розвитку. Як вбачається зі вступних слів Президента України та міністра оборони України, метою її видання є "забезпечення прозорості та відкритості" у вирішенні визначених для Збройних Сил України завдань. У Білій книзі висвітлюється "поточний стан Збройних Сил, а також напрями військового будівництва. У цьому документі достатня увага надається роз'ясненню положень Державної програми розвитку Збройних Сил України на 2006 – 2011 рр. та висвітленню напрямів її виконання" [3, с. 3-6].

У подальшому схожі завдання визначались і в інших щорічних виданнях Білої книги [4 – 8]. Водночас, постановка завдань та дещо публіцистичний характер викладення матеріалів не кореспондувався із висновками фахівців та аналітиків, які в цілому характеризували вкрай негативно вітчизняну військову політику, що знаходилась у постійній кризі в першу чергу через брак фінансування [9; 10, с. 145-147; 11, с. 361].

В аналітичному та науковому опрацюванні досить активно використовувались відомості, оприлюднені у Білих книгах, а дослідники цілком вірно сприймали цю інформацію як офіційну позицію військового керівництва держави.

У подальшому характер викладу інформації в Білих книгах став змінюватись і став відображати в основному позитивно забарвлене звітування конкретних політиків та військових керівників. Так, вступне слово тодішнього керівника Генерального штабу Збройних Сил України до видання Білої книги 2010 року взагалі не містить викладення проблем [8, с. 4-5]. Такий підхід залишався характерним до початку збройної агресії проти України. Зокрема, видання Білої книги 2013 року (датоване 2014 роком) не містить вступного слова військового керівництва взагалі. Водночас констатується, що "у 2013 р. вперше за останні роки на потреби оборони були передбачені видатки менше 1 % ВВП, що не дозволило в повному обсязі забезпечити ресурсні потреби Збройних Сил. Поділ видатків Міністерства оборони за такими напрямами, як утримання Збройних Сил, підготовка військ (сил) та розвиток озброєння і військової техніки, не відповідав класичній світовій моделі і був гіпертрофованим" [12, с. 6]. Також було наведено аналітичні розрахунки розподілу витрат порівняно зі світовою практикою. Окрім цього, досить детально викладались питання організаційної структури військового управління відповідно до нормативно-правових актів та її змін у 2013 році, статистичні дані щодо чисельності Збройних Сил України і динаміки її змін. Окремо проаналізовано стан виконання державних програм, при цьому визначено, що "для виконання заходів з розвитку озброєння та військової техніки у 2013 р. був передбачений фінансовий ресурс, в 1,4 рази менший за показники 2012 р." [12, с 11-12]. Зроблено також аналіз та певні висновки стосовно стану підготовки військ (сил), що, на думку авторів Білої книги, був "високим" хоча і констатовано, що "через обмежене ресурсне забезпечення Збройні Сили не досягли запланованих показників їх польового вишколу" [12, с. 20]. Наведено статистичні дані щодо кадрової політики у Збройних Силах та їх комплектування персоналом, реалізації соціальної та гуманітарної політики, заходів міжнародних зв'язків та участі у миротворчих операціях.

Варто зазначити, що матеріали Білих книг, видані останнім часом, в основному не змінили загальні підходи, що сформувались у попередні роки.

Зокрема, акценти "Білої книги 2014" зроблено на викладенні підсумків реалізації заходів щодо зміцнення обороноздатності держави та участі Збройних Сил в антитерористичній операції. У відповідному контексті проаналізовано окремі питання державної політики в оборонній сфері, зокрема, унормування стратегічного курсу в сфері оборони та удосконалення відповідних правових засад. Детально викладено рішення та заходи, що здійснювались військовим керівництвом держави після початку агресії проти України. Зокрема, "1 березня 2014 р. Збройні Сили були приведені у бойову готовність "ПОВНА", а 17 березня 2014 р. оголошено часткову мобілізацію в Україні" [13, с.9]. Окрім цього, викладено (з наданням статистичних даних) участь Збройних Сил на усіх етапах антитерористичної операції на сході держави у 2014 році. Також детально аналізується стан фінансового забезпечення Збройних Сил (з наведенням відповідних даних), оптимізація структури управління, аналіз зміни чисельності Збройних Сил, стан оснащення озброєнням та військовою технікою,

підготовки військ, комплектування персоналом. Подібна структура з відповідним викладенням зберігалась і у наступних виданнях, статистичні дані при цьому оновлювались для відповідного року [14 – 16].

Таким чином, слід зазначити, що в Міністерстві оборони України процес підготовки та видання Білої книги набув системного характеру, а порядок викладення відомостей відбувається за певною структурою, що склалася у практиці.

Законодавчі вимоги щодо видання зазначених документів для інших суб'єктів сектору безпеки і оборони були відсутні, тому вони видавались не періодично і відображали різні підходи. До 2014 року було видано лише "Білу книгу 2007: Служба безпеки та розвідувальні органи України" і "Білу книгу 2008: Служба безпеки України" [17; 18]. Слід зазначити, що Служба безпеки України періодично надавала звіти в інших формах, що відрізнялись від формату Білої книги [19].

Водночас, розвідувальні органи та деякі інші суб'єкти сектору безпеки і оборони надавали інформацію вкрай дозовано, хоча важливість публічного їх звітування підкреслювалась відповідними фахівцями, оскільки "публічні звіти інформують громадськість про діяльність розвідувальних служб, що сприяє кращому їх розумінню і зміцненню довіри до органів контролю", а також "контролери використовують свої доповіді для спроб ініціювати зміни в розвідувальних службах, у політиці виконавчої влади стосовно розвідки, або у законодавстві, яке регулює діяльність розвідувальних служб. Доповіді органів контролю часто містять рекомендації стосовно покращення певних підходів і практик. Контролери можуть пізніше повертатися до цих рекомендацій, щоб забезпечити відповідальність розвідувальних служб і виконавчої влади за вирішення проблеми в їхній організації, на яку їм вже було попередньо вказано" [20, с. 44]. Іншим важливим аспектом щодо визначення предмету звітування правозахисниками запропоновано вважати надання звітів у розрізі забезпечення прав людини [21].

Але, як свідчить аналіз матеріалів, опублікованих, наприклад, Службою зовнішньої розвідки України на офіційному веб-сайті, для загалу в основному публікуються історичні дослідження, а також мемуари радянських часів.

Окрім цього, Білі книги видаються також як щорічник Національною гвардією України та Державною прикордонною службою України [22]. Структурно зазначені видання подібні до Білих книг, які видаються Міністерством оборони України. Окрім цього, Державна служба спеціального зв'язку та захисту інформації України на своєму офіційному веб-сайті публічну інформацію, наводить під загальною рубрикою "Біла книга".

Водночас варто зауважити, що в інших державах зазначене питання є швидше термінологічним аніж практичним. Зокрема, термін "white paper" (англомовний аналог найменування "Біла книга") стосується особливого виду урядових документів, в яких викладаються засади політики, що відображаються загальні підходи ("філософію") адміністрації і які адресовано громадськості або парламенту [23]. Існує практика видання Білих книг насамперед у випадках необхідності викладення для суспільства важливих засад державної політики. Як правило, такі документи не мають щорічного характеру та ілюструють собою певні зміни (у тому числі на доктринальному рівні) конкретних важливих напрямів державної політики. Прикладом є "Біла книга оборони та національної безпеки Франції" 2013 року [24]. Зазначений документ містить аналіз геостратегічних реалій та відображає загальні підходи до державної політики у сфері оборони та національної безпеки держави. Зрозуміло, що документи подібного характеру не видаються щорічно і у Франції вони видавались у 1972, 1994 та 2008 роках.

У деяких випадках Білі книги видаються на рівні Міністерств оборони або військового керівництва держави. Як приклад слід навести Білі книги Міністерства оборони ФРН та Чеської республіки [25; 26]. У зазначених документах можливо простежити імплементацію стратегічних підходів у діяльності військової організації держави, окрім цього, вони мають і характер звіту про свою діяльність із наведенням відповідних статистичних та аналітичних матеріалів.

Що стосується звітування спеціальних служб (розвідки, контррозвідки), а також правоохоронних органів, то воно відбувається шляхом періодичного (усталеного за часом) оприлюднення відповідних звітів про свою діяльність. Як правило, мова йде про щорічні (за підсумками календарного року) звіти. У науковій літературі час від часу з'являються дослідження стосовно форм і методів громадського (цивільного) контролю за діяльністю спеціальних служб в окремих країнах, при цьому констатовано, що звітування фактично більш притаманне парламентському контролю [27]. На рівні експертів наголошувалось на необхідності та важливості оприлюднення "публічних версій" звітів для спеціальних служб [28, с. 15]. В даному випадку визнається, що оприлюдненню підлягає не весь обсяг звіту про діяльність спеціальної служби, а лише та частина, що може бути оприлюднена.

На сьогодні існує різноманітна практика публічного звітування для спеціальних служб НАТО. Так, наприклад, Поліція безпеки Естонії (Kaitsepolitsei) публікує "щорічні звіти" (review), починаючи з 1998 року, у тому числі англійською мовою. Зазначені звіти у повному обсязі доступні для ознайомлення та отримання електронної копії на офіційному веб-сайті. Як показує аналіз звіту 2017 року, він скоріше відображає погляд Поліції безпеки на політичну ситуацію навколо Естонії, ступінь та характер загроз безпеці та основні напрями протидії. Зазначені висновки підкріплюються відповідними прикладами [29]. Подібна практика характерна і для інших країн Європи, де відповідні спеціальні служби видають "щорічники" (yearbooks), щорічні звіти (annual reports) тощо. Проте зазначена практика характерна далеко не для всіх країн, наприклад Таємна служба Великої Британії надає інформацію шляхом викладення власних цінностей, завдань та напрямів діяльності, також здійснює поточну комунікацію з важливих питань громадської безпеки.

Оновлення спеціального законодавства у сфері забезпечення національної безпеки та оборони в Україні, що відбулось у поточному році, певним чином змінило підходи до інформування суспільства та його відповідних форм. Зокрема, частиною 4 статті 10 Закону України "Про національну безпеку України" передбачено, що "з метою систематичного інформування суспільства про діяльність сектору безпеки і оборони України, забезпечення обґрунтованості рішень державних органів з питань національної безпеки і оборони, про стан виконання заходів розвитку сектору безпеки і оборони періодично, але не рідше ніж раз на три роки, органами сектору безпеки і оборони видаються Білі книги або інші аналітичні документи (огляди, національні доповіді тощо)" [30]. Таким чином, безпосередньо у тексті законодавчого акту як мету видання відповідних матеріалів зазначено "інформування суспільства", причому інформування має бути систематичним. Законодавець, визначивши умову періодичності, відійшов від директивної настанови щорічності видання, яка була визначена Законом України "Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави". Зазначено лише граничний термін – не рідше ніж один раз на три роки. Водночас, суб'єкти сектору безпеки мають самостійно визначати як періодичність (щорічну або іншу) так і форму для аналітичного документу (Біла книга або огляди, національні доповіді тощо).

Частиною 2 статті 12 Закону України "Про національну безпеку України" визначено, що до складу сектору безпеки і оборони входять Міністерство оборони України, Збройні Сили України, Державна спеціальна служба транспорту, Міністерство внутрішніх справ України, Національна гвардія України, Національна поліція України, Державна прикордонна служба України, Державна міграційна служба України, Державна служба України з надзвичайних ситуацій, Служба безпеки України, Управління державної охорони України, Державна служба спеціального зв'язку та захисту інформації України, Апарат Ради національної безпеки і оборони України, розвідувальні органи України, центральний орган виконавчої влади, що забезпечує формування та реалізує державну військово-промислову політику [30].

Як показав проведений вище аналіз, на сьогодні тільки Міністерство оборони України та Національна гвардія України забезпечують щорічне видання Білої книги і здійснюють інформування суспільства про свою діяльність у такій формі. Водночас, оскільки Збройні Сили України та Міністерство оборони України законодавчо вже вважаються різними суб'єктами сектору безпеки і оборони, виникає питання у необхідності для них розподілу компетенції, у тому числі стосовно інформування суспільства. Для інших суб'єктів сектору безпеки практика інформування про свою діяльність у вигляді Білих книг на сьогодні відсутня (за винятком неперіодичних видань Служби безпеки України та Державної прикордонної служби України).

Важливим з огляду на законодавче визначене завдання інформування суспільства про стан виконання заходів розвитку сектору безпеки і оборони постає питання визначення ролі і місця Ради національної безпеки і оборони України та її апарату в підготовці узагальнюючого для всіх суб'єктів сектору безпеки і оборони документа для інформування суспільства. Тим більше, що практика, яка склалась в деяких країнах, надає таким Білим книгам доктринального (для суспільства) значення в сфері безпеки та оборони [24; 25].

Якщо повернутись до вітчизняних реалій, то варто згадати і про нормативно-правові приписи останнього часу стосовно підготовки Білих книг. Зокрема, видання Білих книг визначалось завданнями реформування сектору безпеки і оборони Річними національними програмами підготовки до набуття членства в НАТО та співробітництва "Україна-НАТО" [31 – 33]. При цьому низка останніх нормативно-правових актів містить прямі вказівки для державних органів сектору безпеки стосовно забезпечення щорічного видання Білих книг [34]. Слід зазначити, що фактично щорічне видання таких Білих книг здійснювалося лише Міністерством оборони України і вони стосувались лише діяльності Збройних Сил України, хоча і мали до 2008 року певну зосередженість на питаннях оборонної політики. Зазначена практика була зумовлена прямим законодавчим приписом.

Тому вдосконалення вимог законодавства, з одного боку, більш вдало регламентувало зазначене коло питань, хоча вказані вище законодавчі приписи потребуватимуть додаткових уточнень в компетенції, обсязі необхідних повноважень та практиці правозастосовної діяльності державних органів України з урахуванням існуючого світового досвіду.

Висновки.

1. Започаткована у 2005 році практика щорічного видання узагальнюючого документа інформування громадськості про діяльність окремих суб'єктів сектору безпеки і оборони ("Білої книги") здійснювалась у повному обсязі лише Міністерством оборони України, що зумовлювалось прямими законодавчими приписами. Попри наявність вказівок та розпоряджень, іншими суб'єктами сектору безпеки і оборони інформування шляхом видання Білих книг здійснювалося далеко не періодично.

2. Обсяг, зміст та особливості викладу матеріалу змінювались, водночас спостерігалась тенденція відходу від викладення основ державної політики у певній сфері до звітування (в основному статистичного та ілюстративного характеру) про діяльність конкретних державних органів та їх керівників.

3. Існуюча світова практика свідчить про те, що Біла книга має характер доктринального документу, який не є періодичним і викладає загальні засади державної політики у певній сфері. На рівні міністерства зазначений документ також має скоріше стратегічний характер, аніж просто звіт для громадськості.

4. Щорічне (або інше періодичне звітування) має здійснюватись як одна з форм громадського контролю, а тому конкретні звіти суб'єктів сектору безпеки і оборони повинні викладати інформацію стосовно забезпечення прав і свобод людини, а також реагування на випадки їх порушення з боку представників держави.

5. Подальше розмежування предмету та змісту періодичного інформування шляхом оприлюднення узагальнюючого документу має відбуватись при розробці та впровадженні системи громадського контролю у сфері безпеки і оборони. Особливо важливим є питання суб'єктного складу підготовки та видання основного узагальнюючого документу (Білої книги) у майбутньому.

Використана література

1. Про основи національної безпеки України: Закон України від 19.06.03 р. № 964-IV (*База даних "Законодавство України" / ВР України*). URL: http://zakon.rada.gov.ua/laws/ main/964-15

2. Про демократичний цивільний контроль над Воєнною організацією і правоохоронними органами держави: Закон України від 19.06.03 р. № № 975-IV (*База даних "Законодавство України" / ВР України*). URL: http://zakon.rada.gov.ua/laws/show/975-15

3. Сунгуровський М., Чернова А., Шангіна Л. Біла книга 2005. Оборонна політика України. Київ: Видавництво "Заповіт", 2006. 136 с.

4. Біла книга 2006. Оборонна політика України. Київ: Міністерство оборони України, 2007. 96 с.

5. Біла книга 2007. Оборонна політика України. Київ: Міністерство оборони України, 2008. 120 с.

6. Біла книга 2008. Оборонна політика України. Київ: Міністерство оборони України, 2009. 100 с.

7. Біла книга 2009. Збройні Сили України. Київ: Міністерство оборони України, 2010. 96 с.

8. Біла книга 2010. Збройні Сили України. Київ: Міністерство оборони України, 2011. 84 с.

9. Шеховцов В., Герасимов А., Шаталова О., Куплевацька О. Криза оборонної реформи 2000-2010 років, нові умови, рішення результати: аналітична доповідь ДФ НІСД, 2011. URL: http://www.niss.gov.ua/content/articles/files/Kriza_obor.pdf

10. Турченко Ю. Збройні Сили України: нелінійна еволюція конституційного органу. *Політичний менеджмент*. 2010. № 4. С. 140-148.

11. Терещенко А.М., Копашинський С.А., Марко І.Ю., Терещенко А.М. Деякі проблемні питання державного розвитку Збройних Сил України у 2006-2011 роках та імовірні шляхи їх вирішення. *Вісник Національного університету оборони*. 2013. № 5(36). С. 358-362.

12. Біла книга 2013. Збройні Сили України. Київ: Міністерство оборони України, 2014. 76 с.

13. Біла книга 2014. Збройні Сили України. Київ: Міністерство оборони України, 2015. 85 с.

14. Біла книга 2015. Збройні Сили України. Київ: Міністерство оборони України, 2016. 105 с.

15. Біла книга 2016. Збройні Сили України. Київ: Міністерство оборони України, 2017. 113 с.

16. Біла книга 2017. Збройні Сили України. Київ: Міністерство оборони України, 2018. 152 с.

17. Біла книга 2007: Служба безпеки та розвідувальні органи України ; В.П.Горбулін (ред.). Київ: 2008. 85 с.

18. Біла книга 2008. Служба безпеки України / О.Ф. Бєлов, Д.Г. Анікін, О.С. Власюк та ін. Київ: Ін-т операт. діяльн. та держ. безпеки, 2009. 79 с.

19. Принципи та пріоритети української спецслужби. 2017. URL: https://www.ssu.gov.ua/ua/news/1/category/21/view/3011#.eIkCAPxx.dpbs

20. Віллз А. Розуміння підзвітності розвідки. Женева, DCAF, 2010. 55 с.

21. Захаров Євген. Служба безпеки України та права людини. (Українська гельсінська спілка з прав людини. 23.01.17 р.). URL: https://helsinki.org.ua/sluzhba-bezpeky-ukrajiny-ta-prava-lyudyny-e-zaharov

22. Біла книга Національної гвардії України. URL: http://ngu.gov.ua/ua/bila-knyga-nacional noyi-gvardiyi-ukrayiny

23. Policy Papers and Policy Analysis: Stanford Law School Terms and Definitions. URL: https://www-cdn.law.stanford.edu/wp-content/uploads/2015/04/Definitions-of-White-Papers-Briefing-Books-Memos-2.pdf

24. Livre blanc sur la défense et la sécurité nationale. 2013. URL: http://www.livreblanc defenseetsecurite.gouv.fr/index.html

25. Weiisbuch 2016. Zur Sicherheitspolitik und zur Zukunft der Bundeswehr. URL: https://www. bmvg.de/resource/blob/13708/015be272f8c0098f1537a491676bfc31/weissbuch2016-barrier efrei-data. pdf

26. The White Paper on Defence: 2011. Ministry of Defence of Czech Republic. URL: https://www.eda.europa.eu/docs/default-source/documents/whitepaperondefence2011_1.pdf

27. Система організації управління і правового забезпечення діяльності спецслужб (досвід країн Європейського Союзу та Північної Америки): аналіт. доп. В.Г. Пилипчук, М.О. Будаков, В.М. Гірич. Київ: Національний інститут стратегічних досліджень. 2012. 56 с.

28. Уіллз А. Ефективний демократичний контроль за діяльністю національних служб безпеки: тематична доповідь (оприлюднена Комісаром Ради Європи з прав людини, травень, 2015). URL: http://grafmiville.io/dcaf_2017/web/sites/default/files/publications/documents/CoE_Over sight _Security_Services_ukr.pdf

29. Estonian Internal Security Service: annual review 2016. URL: https://www.kapo.ee/sites /default/files/public/content_page/Annual%20Review%202017.pdf

30. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII (*База даних "Законодавство України" / ВР України*). URL: http://zakon.rada.gov.ua/laws/ main/2469-19

31. Річна національна програма на 2009 рік з підготовки України до набуття членства в Організації Північноатлантичного договору: Указ Президента України від 07.08.09 р. № 600/2009. URL: http://zakon.rada.gov.ua/laws/show/600/2009

32. Річна національна програма на 2010 рік з підготовки України до набуття членства в Організації Північноатлантичного договору: Указ Президента України від 03.02.10 р. № 92/2010. URL: http://zakon.rada.gov.ua/laws/show/92/2010

33. Річна національна програма співробітництва "Україна-НАТО" на 2012 рік: Указ Президента України від 19.04.12 р. № 273/2012. URL: http://zakon.rada.gov.ua/laws/show/273 /2012

34. Річна національна програма під егідою Комісії Україна-НАТО на 2018 рік: Указ Президента України від 28.03.18 р. № 89/2018. URL: http://zakon.rada.gov.ua/laws/ show/89/2018

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

УДК 343.14

ЄВТУШЕНКО Є.В., провідний науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України

ЗАХИСТ ВІД НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ: НОРМАТИВНО-ПРАВОВИЙ ТА ІНФОРМАЦІЙНИЙ АСПЕКТИ

Анотація. *У статті досліджуються юридична природа недобросовісної конкуренції, методи захисту суб'єктів господарювання на товарних ринках, а також питання застосування санкцій за порушення законодавства України про економічну конкуренцію.*

Ключові слова: *захист, недобросовісна конкуренція, господарське законодавство, економіка, суб'єкт господарювання.*

Summary*. The article examines the legal nature of unfair competition, methods of protecting economic entities in commodity markets, as well as the application of sanctions for violating the legislation of Ukraine on economic competition.*

Keywords: *protection, unfair competition, economic legislation, economy, business entity.*

Аннотация. *В статье исследуются юридическая природа недобросовестной конкуренции, методы защиты субъектов хозяйствования на товарных рынках, а также вопросы применения санкций за нарушение законодательства Украины об экономической конкуренции.*

Ключевые слова: *защита, недобросовестная конкуренция, хозяйственное законодательство, экономика, субъект хозяйствования.*

Постановка проблеми. Захист конкуренції є актуальним на сучасному етапі розвитку економіки України. Це пояснюється тим, що, з одного боку, в Україні з'являються нові суб'єкти господарювання, які призводять до загострення конкурентних відносин, а з іншого боку, в Україні майже повністю відсутня корпоративна культура підприємств, наявна в інших провідних країнах. Крім того, питання боротьби з недобросовісною конкуренцією набуває надзвичайної актуальності в сучасній економіці України на етапі її європейської інтеграції.

Добросовісна конкуренція сприяє розвитку і успіху підприємства. Однак, змагання в середовищі суб'єктів господарювання за споживчий попит на ринку може здійснюватися як сумлінно, так і незаконними методами суперництва, що завдає шкоди споживачам, конкурентам та державі в цілому. Йдеться про недобросовісну конкуренцію, яка негативно впливає на розвиток конкурентоспроможності національної економіки на міжнародних ринках. Враховуючи законодавче визначення недобросовісної конкуренції, підприємства для утримання свого ринкового стану змушені виробляти стратегію захисту від неконкурентних дій суперників на ринку, а саме: обирати шляхи захисту, які б забезпечували індивідуалізацію підприємств на товарних ринках.

Результати аналізу наукових публікацій. Проблеми недобросовісної конкуренції та методи захисту від неї досліджують багато науковців, серед яких виділяються праці Бойка А,. Дащенко О., Журика Ю., Слободянюка М. та Панченка М. Проте, поширення недобросовісної конкуренції в сучасних умовах потребує поглиблених наукових

досліджень для розробки комплексу науково-практичних рекомендацій щодо протидії цьому явищу із запровадженням методів захисту суб'єктів господарювання.

Метою статті є розробка пропозицій щодо удосконалення захисту суб'єктів господарювання від негативних проявів недобросовісної конкуренції як економічного явища.

Виклад основного матеріалу. Як зазначається у ст. 42 Господарського кодексу України, підприємницька діяльність є самостійною, ініціативною та систематичною на власний ризик господарською діяльністю, що здійснюється суб'єктами господарювання (підприємцями) з метою досягнення економічних і соціальних результатів та одержання прибутку. У той же час, отримання прибутку – це основна мета підприємця, стратегічним же напрямком його діяльності є збільшення власних капіталів, економічне зростання, що зумовлює прагнення суб'єкта господарювання до пошуку оптимальних економічних рішень для того, щоб вироблені ним товари і послуги мали попит у споживачів. Оскільки в умовах ринку до описаної ситуації прагне кожний суб'єкт підприємницької діяльності, великий прибуток одержить той, хто зробить свій товар конкурентоздатним. У цьому розумінні конкуренція завжди є необхідною умовою підприємницької діяльності в суспільстві, а отже і ринкової економіки, заснованої на товарному виробництві й у публічних закупівлях, в умовах якої суб'єкт господарювання має успішно вести справи шляхом наповнення ринка новим товаром і послугами з подальшим пониженням ціни за одиницю товару.

Що означає конкуренція? З підручників з економічної теорії відомо, що конкуренція – це абстрактна модель, яка може бути інтерпретована як "система невидимок, ведена невидимою рукою". Конкурента система означає, що ніхто з агентів ринку не може мати достатню владу призначати ціну, визначати напрямок розвитку. Конкуренція підтримується демократичними інститутами та громадянським суспільством, а конкурентні ринки забезпечують найбільш важливі засоби довготривалого економічного розвитку. Створення перешкод конкуренції в економіці скорочує інновації, порушує механізм вироблення перспективних ідей [1].

Зрозуміло, що діяльність суб'єктів господарювання повинна бути ефективною і корисною. По-перше, суб'єкт господарювання особисто зацікавлений у своїй справі, тому він використовує свої знання для розширення масштабів власного бізнесу і завдяки цьому має більше шансів досягти успіху. По-друге, суб'єкт господарювання може швидше і з меншими зусиллями задовольняти суспільні потреби і ринковий попит, оскільки завжди намагається передбачити цей попит ще на стадії формування цін, завдяки цьому може отримати певні знижки раніше, чим його конкуренти. По-третє, діяльність підприємця сприяє задоволенню ринкового попиту, що утворюється з меншими втратами для суспільства [2] .

Викладене зумовлює потребу чіткого визначення правового статусу підприємця, тобто його прав, обов'язків та відповідальності. Особливого визначення "правовий статус підприємця" набуває в умовах євроінтеграції України в контексті її економічних реформ. Відомо, що для того, щоб вийти на ринок ЄС з конкурентоспроможною продукцією та здійснювати ефективну рентабельну діяльність, необхідно в національному законодавстві чітко окреслити права та обов'язки суб'єктів підприємницької діяльності [3].

З метою забезпечення свободи розвитку підприємства, встановлення правових гарантій його функціонування сьогодні вже визначені окремі права, обов'язки, а також регламентовано відповідальність суб'єктів господарювання. Зокрема, чинне законодавство передбачає, що для реалізації господарської ініціативи підприємець має право здійснювати такі дії:

- створювати для проведення підприємницької діяльності будь-які види підприємства;
- купувати повністю або частково майно та набувати майнового права;
- самостійно формувати господарську діяльність, обирати постачальників та споживачів, встановлювати ціни і тарифи, вільно розпоряджатися прибутком;
- укладати з громадянами трудові договори щодо використання їхньої праці (контракти, угоди);
- самостійно визначати форми, системи і розміри оплати праці та інші види доходів осіб, що працюють за наймом;
- отримувати будь-який необмежений за розмірами власний дохід;
- брати участь у зовнішньоекономічних відносинах, здійснювати валютні операції;
- отримувати будь-який необмежений за розмірами власний дохід тощо.

Права суб'єктів господарювання можна класифікувати відповідно до їхнього змісту:

- засновницькі права – включають право на вільний вибір засновниками видів діяльності, право на вибір організаційно-правової форми, право на прийняття рішення про створення "припинення" діяльності підприємства;
- права в галузі управління – самостійно визначати структуру підприємства, ухвалювати і змінювати установчі документи, затверджувати положення про структурні підрозділи, формувати органи управління і контролювати їхню діяльність, призначати посадових осіб;
- майнові права – є речовим правом суб'єкта підприємця, на володіння, розпорядження та використання основних фондів, обігових коштів, інших цінностей, вартість яких відображається на самостійному балансі підприємства, ведення господарської та комерційної діяльності, а також представляти інтереси у судових органах.

Одним із основних напрямів діяльності держави для забезпечення реалізації прав підприємців є захист економічної конкуренції.

Добросовісна конкуренція примушує виробників підвищувати якість продукції (товарів, робіт та послуг) прискорювати впровадження новітніх досягнень науки та техніки для отримання більшого прибутку та переваг над іншими конкурентами.

Правову основу захисту економічної конкуренції складають закони України "Про захист економічної конкуренції"; "Про Антимонопольний комітет"; "Про захист від недобросовісної конкуренції"; "Про природні монополії"; "Про публічні закупівлі".

Закон України "Про захист економічної конкуренції" визначає економічну конкуренцію як змагання між суб'єктами господарювання з метою здобуття, завдяки власним досягненням, переваг над іншими суб'єктами господарювання, внаслідок чого споживачі, суб'єкти господарювання мають можливість вибирати між кількома продавцями, а окремий суб'єкт господарювання не може визначати умови обігу товарів на ринку.

Відповідно до законодавчого визначення недобросовісної конкуренції захист від такого виду конкуренції розуміється як врегульована законом діяльність держави, її органів і посадових осіб, що контролюють процес конкуренції, учасників конкуренції, спрямована на встановлення елементів матеріально-правового відношення, що виникло внаслідок порушення конкуренції у підприємницькій діяльності, а також припинення недобросовісної конкуренції шляхом притягнення винних до відповідальності. Формами недобросовісної конкуренції є:

- неправомірні дії, спрямовані на отримання певних переваг над конкурентом за рахунок його інтелектуальної діяльності та ділової репутації;

- неправомірні дії, пов’язані з дезорганізацією виробничого процесу конкурента, створенням йому перешкод під час конкурентної боротьби та досягненням неправомірних переваг у конкуренції;
- дії, пов’язані з неправомірним збиранням, розголошенням та використанням комерційної таємниці [10].

Захист від недобросовісної конкуренції визнається складовою системи охорони промислової власності для країн, що розвиваються. 12 видів діяльності зараховані до недобросовісної конкуренції:

- підкуп покупців конкурента з метою створення групи зацікавлених осіб з боку покупців;
- промислове шпигунство чи підкуп службовців конкурента з метою розвідування ділової або комерційної таємниці;
- використання чи розкриття без дозволу зведеного технічного “ноу-хау” конкурента;
- підштовхування службовців конкурента до порушення договорів з найму чи до звільнення з роботи;
- погроза на адресу конкурентів подати позов за порушення патенту чи товарного знака, якщо така погроза робиться недобросовісно з метою скорочення товарного обігу конкурента чи створення йому перешкод;
- бойкотування торгівлі для перешкоди конкуренції або її запобігання;
- демпінг, тобто продаж дешевше собівартості, з метою перешкодити конкуренції, якщо демпінг призводить саме до такого наслідку;
- створення враження, що пропонуються надзвичайно сприятливі умови покупки, якщо це не відповідає дійсності;
- піратське копіювання товарів, послуг, реклами та інших характеристик комерційної діяльності конкурента;
- заохочення конкурента до невиконання контракту;
- реклама, що містить порівняння з товарами чи послугами конкурента;
- порушення положень законів, що не мають прямого відношення до конкуренції, з метою одержання шляхом такого порушення несумлінної переваги над іншими конкурентами [11].

Водночас, органи державної влади повинні в рамках своїх повноважень сприяти розвитку конкуренції, але на практиці це відбувається не завжди, оскільки іноді зумовлені корупцією протиправні дії посадових осіб державних органів певним чином обмежують конкуренцію.

Захист інтересів споживачів є одним з головних наслідків боротьби з недобросовісною конкуренцією, оскільки саме кінцевий споживач у підсумку відчуває на собі ефективність функціонування економіки та наслідки недобросовісної конкуренції. Враховуючи зазначені вище передумови, виділяють такі цілі захисту інтересів суб’єктів господарювання від недобросовісної конкуренції [3]:

- забезпечення рівності суб’єктів господарювання під час здійснення підприємницької діяльності;
- захист суб’єктів господарювання від проявів недобросовісної конкуренції на внутрішньому/зовнішньому ринках;
- запобігання можливостям досягнення неправомірних переваг у конкуренції;
- захист інтелектуальної власності на зовнішньому та внутрішньому ринках;
- забезпечення реалізації споживачами своїх прав на гарантований рівень споживання, відповідну якість товарів тощо.

Серед основних методів недобросовісної конкуренції виділяють: економічне (промислове) шпигунство, підробку продукції конкурентів, підкуп і шантаж, обдурювання споживачів, махінації з діловою звітністю, валютні махінації, приховування дефектів тощо [2]. Крім того, в умовах розвитку глобалізації та прагнення України до інтеграції в європейські економічні структури питання захисту від недобросовісної конкуренції та конкурентної політики в цілому набуває нового змісту. Уповноваженими органами, які здійснюють захист від недобросовісної конкуренції, є суди України, Антимонопольний комітет та правоохоронні органи. Зауважимо, що на рівні держави методи захисту від недобросовісної конкуренції можуть використовуватися, в першу чергу, Антимонопольним комітетом України.

Одним із методів захисту від недобросовісної конкуренції є здійснення підприємством антимонопольної діяльності, тобто діяльності окремих суб'єктів господарювання (юридичних та фізичних осіб), яка спрямована на створення та підтримку конкурентного середовища, зокрема, конкурентних відносин, на певному товарному ринку через протидію неконкурентній діяльності монопольних утворень. Ступінь використання підприємством методів захисту залежить не тільки від внутрішнього середовища компанії, але також і від зовнішнього середовища, оскільки захист від недобросовісної конкуренції, хоча здійснюється в середині підприємства, але результати його використання проявляються у зовнішньому середовищі, зокрема, до контрагентів підприємства [2].

Згідно зі ст. 37 Господарського кодексу України вчинення дій, визначених як недобросовісна конкуренція, зумовлює адміністративну, цивільну чи кримінальну відповідальність винних осіб суб'єктів господарювання у випадках передбачених законом [1].

У сфері економічних відносин, захист конкуренції забезпечується різними способами, у тому числі заходами правого впливу в рамках юридичної відповідальності, що є предметом окремого дослідження.

Якщо звернутися до позитивного зарубіжного досвіду суміжних з Україною держав, то слід відзначити, що, наприклад, у Польщі після вступу до Європейського Союзу відбулась гармонізація антимонопольного законодавства цієї країни з нормами ЄС, а новий антимонопольний орган почав діяти в рамках Європейської конкурентної мережі (ECN). Відповідно до Регламенту комісії (ЄС) № 802/2004 від 07.04.2004 р. щодо контролю за концентрацією суб'єктів господарювання Європейська Комісія має право проводити розслідування концентрації у "Вимірі Союзу". У зв'язку з цим у Польщі 16 лютого 2007 року був прийнятий новий Закон "Про захист конкуренції і прав споживачів" [8].

Цей Закон спростив процедуру порушення справ на підставі дій, що обмежують конкуренцію і порушують колективні інтереси споживачів. Закон обмежує суму штрафу за порушення (наприклад, зловживання домінуючим положенням на ринку, проведення концентрації без попереднього дозволу Голови антимонопольного органу або посягання на колективні інтереси споживачів) 10 % від річного фінансового обороту компанії у попередньому році. Закон наділяє Голову антимонопольного органу повноваженнями накладати штраф у разі якщо підприємство: надало неправдиві відомості у заяві на оформлення угоди про концентрацію; не надало інформацію, коли цього вимагало Управління; надало неправдиву інформацію або таку, що вводить в оману антимонопольний орган. Сума штрафу може в такому випадку сягати до 50 млн. Євро. Крім того, штраф у розмірі до 10 тис. Євро може бути призначено за кожен день

прострочення у реалізації порушення Закону “Про захист конкуренції і прав споживачів” та юридично обов’язкових судових рішень.

Висновки.

Антимонопольне законодавство забезпечує захист ринкової конкуренції, зміст якої полягає у реалізації творчої, стимулюючої та регуляторної функції.

На наш погляд, удосконаленню національного антимонопольного законодавства сприятиме створення відкритого реєстру суб’єктів недобросовісної конкуренції, оптимізація відповідальності за прояви недобросовісної конкуренції шляхом збільшення розмірів штрафів за це діяння.

Створення єдиної внутрішньої узгодженої системи регулювання добросовісних конкурентних відносин є необхідною умовою ефективного функціонування і розвитку ринкової економіки в Україні.

Використана література

1. Норт Д., Уоллис Д., Вайнгаст Б. Насилие и социальные порядки. Москва: Изд-во института Гайдара, 2011. 518 с.

2. Бойко А. Методи захисту від недобросовісної конкуренції. URL: http://www.conf-cv.at.ua/forum/12-27-1 (заголовок з екрану).

3. Журик Ю. Поняття та види недобросовісних дій у конкуренції. *Підприємство, господарство та право*. 2000. № 2. С. 11-16.

4. Про Антимонопольний комітет: Закон України від 26.11.93 р. № 3659-XII. URL: http://www.zakon.rada.gov.ua/laws/show/3659-12 (заголовок з екрану).

5. Про захист економічної конкуренції: Закон України від 11.01.01 р. № 2210-III. URL: http://www.zakon.rada.gov.ua/go/2210-14 (заголовок з екрану).

6. Про захист від недобросовісної конкуренції: Закон України від 07.06.96 р. № 236/96-ВР. URL: http://www.zakon.rada.gov.ua/go/236/96 (заголовок з екрану).

7. Про природні монополії: Закон України від 20.04.00 р. № 1682-III. URL: http://www.zakon2.rada.gov.ua/laws/show/ 1682-14 (заголовок з екрану).

8. Про контроль за концентрацією суб’єктів господарювання: Регламент Комісії ЄС № 802/2004 від 07.04.04 р., з імплементацію Регламенту Ради (ЄС) № 139/2004. *Офіційний вісник Європейського Союзу*. 2004. № 133/1. С. 4-9.

9. Панченко М. Добросовісність, розумність, справедливість, правові засади цивільного права України. URL: http://lib.sumdu.edu.ua/library/TopicDescription?topic_id (заголовок з екрану).

10. Слободянюк М. Добросовісна конкуренція – законні норми поведінки. *Вісник АМКУ*. 2006. № 2. С. 52-55.

11. Цибульов П. Основи інтелектуальної власності 2005. URL: http://www. bookz.com.ua/23 (заголовок з екрану).

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

УДК 342.9

ТКАЧУК Н.А., *кандидат юридичних наук,*
старший науковий співробітник НДІІП НАПрН України

ПРАВОВЕ РЕГУЛЮВАННЯ ВЗАЄМОДІЇ СЛУЖБИ БЕЗПЕКИ УКРАЇНИ З ПРИВАТНИМ СЕКТОРОМ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Анотація. *У статті автор досліджує основні проблемні питання правового регулювання взаємодії СБ України з приватним сектором у сфері забезпечення кібербезпеки та пропонує шляхи їх вирішення.*

Ключові слова: *кібербезпека, державно-приватне партнерство, державно-приватна взаємодія, правове регулювання, Служба безпеки України.*

Summary. *In this article the author investigates the main problematic issues of legal regulation of the cooperation between the Security Service of Ukraine and private sector in the field of cyber security and suggests ways of their solution.*

Keywords: *cyber security, public-private partnership, public-private interaction, legal regulation, Security Service of Ukraine.*

Аннотация. *В статье автор исследует основные проблемные вопросы правового регулирования взаимодействия СБ Украины с частным сектором в сфере обеспечения кибербезопасности и предлагает пути их решения.*

Ключевые слова: *кибербезопасность, государственно-частное партнерство, государственно-частное взаимодействие, правовое регулирование, Служба безопасности Украины.*

Постановка проблеми. Актуалізація кіберзагроз національній безпеці та перетворення кібервпливу на інструмент терористичної, а також розвідувально-підривної діяльності спецслужб іноземних країн проти нашої держави обумовлює потребу посилення кібербезпекових спроможностей Служби безпеки України, як одного із ключових суб'єктів національної системи кібербезпеки, який вирішує завдання із протидії вказаним загрозам.

Важливою умовою підвищення потенціалу вітчизняної спецслужби є забезпечення ефективної взаємодії з приватним сектором. Ключова роль державно-приватного партнерства обумовлена специфікою кібербезпекової сфери. Наразі, кібербезпека є єдиною сферою національної безпеки, яка настільки тісно пов'язана із приватним сектором – по-перше, значний обсяг об'єктів кібербезпеки та кіберзахисту перебуває у приватній власності, по-друге, механізм поширення кіберзагроз в мережі Інтернет фактично нівелює різницю між державними та приватними суб'єктами, по-третє, найбільш досвідчені експерти з ІТ-безпеки працюють саме у недержавному секторі.

Безумовно, розбудова дієвих механізмів державно-приватного партнерства у контексті діяльності СБУ вимагає створення належної правової бази, яка б сприяла залученню громадянського суспільства до забезпечення кібербезпеки держави.

Результати аналізу наукових публікацій. Сутність, організаційно-правові засади та проблемні питання державно-приватного партнерства у сфері кібербезпеки розглядалися у наукових працях В. Бойко, Н. Буша, О. Гівена, С. Гнатюка, Д. Дубова, М. Карр, В. Круглова, М. Ожевана та інших вітчизняних і закордонних вчених. Водночас, на сьогодні відсутні наукові роботи, присвячені дослідженню проблематики нормативного регулювання такого партнерства у контексті діяльності Служби безпеки України, що обумовлює актуальність теми статті.

Метою статті є дослідження сучасного стану правового регулювання партнерства СБ України з приватним сектором у сфері забезпечення кібербезпеки, визначення основних проблемних питань та розробка рекомендацій із удосконалення чинного законодавства у вказаній сфері.

Виклад основного матеріалу. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" на Службу безпеки України покладено ряд важливих завдань у сфері кібербезпеки, серед яких: боротьба з кібертероризмом та кібершпигунством, протидія кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави, розслідування кіберінцидентів та кібератак щодо критичної інформаційної інфраструктури, реагування на кіберінциденти у сфері державної безпеки та інші [1].

Посилення спроможностей Служби безпеки для ефективної протидії цим загрозам визначається Концепцією розвитку сектору безпеки і оборони України як один із пріоритетних напрямів реформування відомства [2]. Безумовно, підвищення ефективності діяльності СБ України у сфері кібербезпеки неможливе без належної взаємодії з приватним сектором. Відповідно до чинного законодавства принцип державно-приватної взаємодії є одним із основоположних принципів забезпечення кібербезпеки України, який в першу чергу повинен реалізовуватись "шляхом обміну інформацією про інциденти кібербезпеки" [1].

З метою розвитку державно-приватного партнерства для запобігання кіберзагрозам, реагування на кібератаки та кіберінциденти у сфері державної безпеки та усунення їх наслідків Службою безпеки України вживаються системні заходи щодо залучення громадянського суспільства до протидії кіберзагрозам національній безпеці.

Так, фахівцями Ситуаційного центру забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform) створено систему збору і обробки інформації щодо інцидентів кібербезпеки та обміну технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури між суб'єктами сектору безпеки в режимі реального часу MISP-UA (Ukrainian Advantage). Ця платформа широко використовується в усьому світі, а також відповідає міжнародним стандартам ЄС та НАТО і застосовується основними міжнародними суб'єктами у сфері кібербезпеки: FIRST, CIRCL, CiviCERT, NATO NCI Agency [3].

Правовою основою інформаційного обміну з використанням інструментів MISP-UA є Меморандум про взаємодію, в рамках якого Службою безпеки України налагоджено обмін інформацією про кіберінциденти та ідентифікатори компрометації з низкою об'єктів критичної інфраструктури приватного сектору (у т.ч. у сфері енергетики, транспорту, телекомунікацій, банківській сфері, оборонній промисловості тощо), а також провідними корпораціями у сфері кібербезпеки [4; 5].

Своєчасний обмін такою інформацією дозволяє завчасно попередити та локалізувати кібератаки, підвищує ефективність реагування з боку СБУ на атаки високого ступеня складності. Слід зазначити, що упереджувальна інформація про можливі кібератаки надається приватному сектору саме з боку Служби безпеки України, що сприяє підвищенню захищеності критичної інфраструктури.

Вказані організаційно-правові заходи свідчать про розуміння керівництвом Служби безпеки важливості налагодження партнерства з приватним сектором та готовність надавати допомогу бізнесу щодо протидії кіберзагрозам. Як заявив голова СБУ Василь Грицак, підкреслюючи надпріоритетність такої взаємодії – "Будь-який

представник великого, середнього та навіть малого бізнесу може звернутися до Ситуаційного центру забезпечення кібербезпеки за консультаціями та допомогою" [6].

Іншим перспективним напрямом державно-приватної взаємодії є залучення ІТ-фахівців приватного сектору (т.зв. "активістів") до проведення негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів, що є одним із функціональних завдань СБ України.

Виявлення вразливостей в інформаційно-телекомунікаційних системах об'єктів критичної інформаційної інфраструктури ("пентестінг") є важливою задачею і цілком підпадає під сутнісні ознаки державно-приватної взаємодії. Проте, така діяльність потребує створення відповідного правового поля. На сьогодні, проведення негласного пентестінгу формально містить ознаки складу злочину, передбаченого статтею 361 Кримінального кодексу України "Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку". Формулювання зазначеної статті КК Украни фактично унеможливлює діяльність некомерційних пентестерів, якщо ці тести заздалегідь не погоджені із об'єктами атаки [7, с. 66].

Першим кроком на шляху модернізації вітчизняного законодавства має бути створення відповідного правового поля для здійснення "хактивістами" пентестової діяльності в інтересах негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів у спосіб, який би не наносив шкоду державній безпеці. Вважаємо, що вказана діяльність має бути попередньо узгоджена із Службою безпеки України, до компетенції якої належить проведення негласних перевірок, що власне і буде підставою для легалізації таких дій.

У вітчизняних наукових колах існує думка, що механізм легалізації пентестінгу повинен полягати у застосуванні правового інституту звільнення від кримінальної відповідальності (наприклад, Д. Дубов пропонує доповнити статтю 361 КК України наступним пунктом: "звільняється від кримінальної відповідальності громадянин України, якщо таке втручання здійснювалось за погодженням із суб'єктами національної системи кібербезпеки…"[7, с. 79]).

Водночас, відповідно до роз'яснення Верховного Суду України [8], звільнення від кримінальної відповідальності – це відмова держави від застосування щодо особи, котра вчинила злочин, установлених законом обмежень певних прав і свобод шляхом закриття кримінальної справи. Причому звільнення від кримінальної відповідальності, відповідно до ч. 2 статті 44 КК України, здійснюється виключно судом. Так, відповідно до Розділу ІХ "Звільнення від кримінальної відповідальності" його підставами можуть бути: дійове каяття (ст. 45), закінчення строків давності (ст. 49), передача особи на поруки (ст. 47) та ін. [9].

Вважаємо, що залучення Службою безпеки осіб в рамках державно-приватної взаємодії до негласної перевірки стану кіберзахисту об'єктів критичної інфраструктури в інтересах національної безпеки повинне бути обставиною, яка не лише звільняє від кримінальної відповідальності, а взагалі виключає злочинність діяння.

Тому пропонуємо доповнити статтю 361 КК України наступним пунктом: "Не є злочином дії особи, передбачені частиною першою цієї статті, яка відповідно до закону виконувала спеціальне завдання органів державної безпеки із негласної перевірки готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів". Це дозволить створити правове поле для розвитку державно-приватної взаємодії за вказаним напрямом.

Важливим напрямом державно-приватного партнерства у сфері протидії кіберзагрозам є взаємодія з Інтернет-провайдерами. Незважаючи на те, що ролі правоохоронних органів та операторів і провайдерів телекомунікацій є різними – правоохоронні органи протидіють злочинності, в той час як постачальники послуг забезпечують користувачам можливість спілкування – необхідно виробити такий механізм взаємодії, який би робив кіберпростір безпечнішим і в той же час забезпечував повагу до різних ролей суб'єктів взаємодії, а також прав та свобод користувачів [10].

На сьогодні проблемним питанням залишається відсутність ефективного правового механізму щодо отримання в інтересах забезпечення національної безпеки від операторів та провайдерів телекомунікацій комп'ютерних даних, необхідних для своєчасного реагування на кіберзагрози, у т.ч. попередження і локалізації кіберінцидентів та кібератак на критичну інформаційну інфраструктуру.

До таких даних належить інформація технологічного характеру щодо дій абонентів (дані про з'єднання, лог-файли, IP-адреси тощо), а також відомості, які можуть ідентифікувати їх особу, за винятком контенту (змістовного наповнення інформаційних потоків).

Своєчасне отримання комп'ютерних даних від провайдера у багатьох випадках дозволяє встановити особу злочинця, виявити механізм поширення шкідливого програмного забезпечення (далі – ШПЗ), а також виявити інші інфіковані зазначеним ШПЗ комп'ютерні мережі, що дозволяє вчасно локалізувати поширення вірусу та попередити масовані кібератаки на критичну інфраструктуру держави, а також кібершпигунство щодо інформації, яка циркулює в державних електронних інформаційних ресурсах.

Відповідно до статей 16 – 18 Конвенції Ради Європи про кіберзлочинність [11], яка є основним міжнародним нормативно-правовим актом у сфері кібербезпеки та була ратифікована Україною в 2005 році, кожна Сторона повинна вжити законодавчих та інших заходів, необхідних для забезпечення термінового збереження та розкриття постачальником послуг на вимогу компетентного правоохоронного органу даних про рух інформації, а також комп'ютерних даних, що не є власне даними змісту інформації, за допомогою яких можна встановити:

- тип комунікаційної послуги, яка використовувалася, її технічні положення і період користування послугою;
- особистість користувача послуг, поштову або географічну адресу, телефони та інший номер доступу, інформацію про рахунки і платежі, яку можна отримати за допомогою угоди про постачання послуг;
- будь-яку іншу інформацію про місце встановлення комунікаційного обладнання, яку можна отримати за допомогою угоди про постачання послуг.

Норми національного законодавства (частини 2, 5 ст. Закону України "Про контррозвідувальну діяльність" [12], частина 3 ст. 25 Закону України "Про Службу безпеки України" [13], ст. 11 Закону України "Про основні засади забезпечення кібербезпеки України" [1], частина 6 ст. 6 та частина 1 ст. 25 Закону України "Про захист персональних даних" [14]) також забезпечують СБ України законні підстави звертатися до операторів та провайдерів телекомунікацій з запитами щодо надання відповідних комп'ютерних даних в інтересах забезпечення національної та кібербезпеки держави.

Водночас, як свідчить практика діяльності підрозділів СБ України, деякі оператори та провайдери телекомунікацій ігнорують законні вимоги органів СБ України та не надають таку інформацію на запити Служби [15; 16], незважаючи на норми законодавства.

В результаті Служба безпеки України не може своєчасно отримати інформацію, необхідну для протидії кіберзагрозам національній безпеці, та фактично не має жодного інструменту впливу на вказаних суб'єктів господарювання через відсутність в законодавстві будь-якої відповідальності, передбаченої за невиконання законних вимог представників СБ України.

Абсурдність ситуації підкреслює той факт, що Кодекс України про адміністративні правопорушення (Глава 15) [17] встановлює адміністративну відповідальність за невиконання законних вимог посадових осіб переважної більшості державних органів: НАБУ, Нацполіції, органів прокуратури, Держспецзв'язку, НКРЗІ, Держфінмоніторингу, Рахункової палати, Держпродспоживслужби, Держпраці, Держатомрегулювання, Укрдержархіву, народних депутатів України, інспекторів сільського господарства, державних фітосанітарних інспекторів та багатьох інших. Відсутність у цьому переліку посадових осіб Служби безпеки України не тільки значно зменшує спроможності СБУ із протидії загрозам державній безпеці, але й певною мірою підриває авторитет національної спецслужби.

Таким чином, існує потреба доповнення Кодексу України про адміністративні правопорушення відповідною нормою, яка б передбачала встановлення адміністративної відповідальності за невиконання законних вимог посадових осіб Служби безпеки України.

Не можна не погодитись з М. Карр, яка, аналізуючи міжнародний досвід щодо налагодження державно-приватного партнерства у сфері кібербезпеки, доходить до висновку, що успішне державно-приватне партнерство може ґрунтуватися або на спільних інтересах або ж, якщо інтереси партнерів не збігаються, на чітких законодавчо закріплених вимогах [18].

Окремо слід відзначити проблемне питання організації збереження операторами та провайдерами надання телекомунікацій послуг даних, щодо записів про надані телекомунікаційні послуги протягом строку позовної давності, визначеного законом.

Відповідно до ст. 39 Закону України "Про телекомунікації" [19] оператори і провайдери телекомунікацій зобов'язані зберігати інформацію щодо наданих телекомунікаційних послуг, однак відсутність у законодавстві чіткого визначеного переліку відомостей, що підлягає збереженню, не дозволяє створити дієвий механізм контролю за виконанням цієї норми Закону, а також одержувати співробітниками правоохоронних органів, у повній мірі, даних (потенційних електронних доказів), необхідних для запобігання, виявлення та припинення кіберзагроз, розслідування кіберінцидентів та кібератак.

Крім того, негативно впливає на стан взаємоді неврегульованість використання провайдерами телекомунікаційних послуг механізму перетворення мережевих адрес за технологією NAT (Network Address Translation).

Застосування зазначеної технології дозволяє провайдерам заощадити ресурс IP-адрес шляхом трансляції декількох внутрішніх IP-адрес в одну зовнішню публічну IP-адресу. Водночас, використання цієї технології без обов'язкового логування (фіксації службової та статистичної інформації про події в комп'ютерній системі) унеможливлює або ускладнює процес ідентифікації злочинців в мережі Інтернет. Ця проблема є актуальною не лише для України. У минулому році Європол офіційно звернувся до провайдерів та операторів телекомунікацій із вимогою припинити використання зазначеної технології [20].

Таким чином, виникає нагальна потреба у розробці нормативно-правового акту, що дозволить конкретизувати види необхідної для розслідування кіберінцидентів і

кіберзлочинів технологічної інформації, що супроводжує сеанси телекомунікаційного зв'язку, визначить терміни та обсяги її зберігання постачальниками телекомунікаційних послуг, а також врегулює порядок надання цієї інформації правоохоронним органам на різних стадіях запобігання злочинів та кримінального переслідування злочинців, та в свою чергу, вирішить питання деанонімізації корисувачів мережі Інтернет, яким надано доступ за технологією NAT.

Залишаються неузгодженими у розрізі регулювання державно-приватного партнерства у сфері кібербезпеки положення законів України "Про державно-приватне партнерство" [21] та "Про основні засади забезпечення кібербезпеки України" [1], що негативно впливає на формування правової основи такого партнерства не лише у контексті діяльності Служби безпеки України, а і всіх суб'єктів національної кібербезпекової системи. Зокрема, на законодавчому рівні слід врегулювати наступні проблемні питання:

- чітко визначити взаємовідношення державно-приватного партнерства та державно-приватної взаємодії у сфері кібербезпеки. Зокрема, чи є така взаємодія різновидом державно-приватного партнерства, та відповідно, чи підпадає під дію Закону України "Про державно-приватне партнерство";

- передбачити внесення до переліку сфер застосування державно-приватного партнерства, визначених у статті 4 Закону України "Про державно-приватне партнерство", сферу кібербезпеки та кіберзахисту;

- враховуючи, що відповідно до положень чинного законодавства [21], [22] головним органом виконавчої влади, що забезпечує формування і реалізацію державної політики щодо державно-приватного партнерства є Мінекономрозвитку, необхідно визначити роль вказаного державного органу у формуванні та реалізації державної політики щодо державно-приватного партнерства у сфері кібербезпеки. З урахуванням того, що Мінекономрозвитку не є основним суб'єктом національної системи кібербезпеки [1], можливо передбачити покладення вказаних обов'язків на одного із ключових суб'єктів такої системи.

Висновки.

Дослідження правових основ партнерства СБ України з приватним сектором у сфері забезпечення кібербезпеки дає змогу дійти таких основних висновків і пропозицій:

1. Забезпечення дієвої взаємодії з приватним сектором є важливою умовою ефективного виконання Службою безпеки України завдань у сфері кібербезпеки, що обумовлено як специфікою кібербезпекової сфери, так і загальносвітовою тенденцією щодо зростання ролі державно-приватного партнерства у діяльності правоохоронних органів.

2. На сьогодні ключовим напрямом такого партнерства є обмін у режимі реального часу інформацією технічного характеру про кіберзагрози з об'єктами критичної інфраструктури приватного сектору та надання допомоги Ситуаційним центром забезпечення кібербезпеки СБУ у локалізації кіберінцидентів та кібератак на такі об'єкти.

3. З метою подальшої розбудови організаційно-правових засад партнерства СБ України з приватним сектором та удосконалення правової основи такої взаємодії пропонується:

- врегулювати на законодавчому рівні залучення ІТ-фахівців приватного сектору (т.зв. "хактивістів") до проведення негласних перевірок готовності об'єктів критичної інфраструктури до можливих кібератак та кіберінцидентів шляхом внесення відповідних змін до статті 361 КК України;

- забезпечити імплементацію у національне законодавство положень Конвенції Ради Європи про кіберзлочинність у частині забезпечення термінового збереження та розкриття постачальником телекомунікаційних послуг на вимогу компетентного правоохоронного органу даних про рух інформації та інших комп'ютерних даних;

- розробити нормативно-правовий акт, що дозволить конкретизувати види необхідної для розслідування кіберінцидентів і кіберзлочинів технологічної інформації, що супроводжує сеанси телекомунікаційного зв'язку, визначить терміни та обсяги її зберігання постачальниками телекомунікаційних послуг, а також врегулює порядок надання цієї інформації правоохоронним органам на різних стадіях запобігання злочинів та кримінального переслідування злочинців;

- доповнити Кодекс України про адміністративні правопорушення нормою, яка б передбачала встановлення адміністративної відповідальності за невиконання законних вимог посадових осіб Служби безпеки України;

- врегулювати питання деанонімізації корисувачів мережі Інтернет, доступ яким надано за технологією NAT;

- узгодити у розрізі регулювання державно-приватного партнерства у сфері кібербезпеки положення законів України "Про державно-приватне партнерство" та "Про основні засади забезпечення кібербезпеки України".

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. URL: http://zakon.rada.gov.ua/laws/show/2163-19

2. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року "Про Концепцію розвитку сектору безпеки і оборони України": Указ Президента України від 14.03.16 р. № 92. URL: https://www.president.gov.ua/documents/922016-19832

3. СБУ розширює співпрацю з громадськістю у рамках розвитку державно-приватного партнерства. URL: https://upmp.news/ua-in-ukraine/sbu-rozshiryuye-spivpratsyu-z-gromadkistyu-u-ramkah-rozvitku-derzhavno-privatnogo-partnerstva

4. СБУ і "Антонов" підписали меморандум щодо обміну даними про кібератаки в режимі реального часу. URL: https://ua.interfax.com.ua/news/general/517243.html

5. СБУ посилює захист інформаційної безпеки підприємств енергетичної галузі України. URL: https://ssu.gov.ua/ua/news/1/category/2/view/5213#.9yybILHi.dpbs

6. Голова СБУ відкрив Ситуаційний центр забезпечення кібернетичної безпеки. URL: https://ssu.gov.ua/ua/news/1/category/21/view/4318#.htoMBif9.dpbs

7. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с.

8. Про практику застосування судами України законодавства про звільнення особи від кримінальної відповідальності: Постанова пленуму Верховного суду України від 23.12.05 р. № 12.

9. Кримінальний кодекс України: Закон України. URL: http://zakon.rada.gov.ua/laws/show/2341-14/print

10. Law enforcement – Internet service provider Cooperation. URL: https://www.coe.int/ru/web/cybercrime/lea-/-isp-cooperation

11. Про ратифікацію Конвенції про кіберзлочинність: Закон України 7.09.05 р. № 2824-IV. URL: http://zakon.rada.gov.ua/laws/show/2824-15

12. Про контррозвідувальну діяльність: Закон України від 6.12.02 р. № 374-IV. URL: http://zakon.rada.gov.ua/laws/show/374-15

13. Про Службу безпеки України: Закон України від 25.03.92 р. № 2229-XII. URL: http://zakon.rada.gov.ua/laws/show/2229-12

14. Про захист персональних даних: Закон України від 2010 р. URL: http://zakon.rada.gov.ua/laws/show/2297-17

15. Представники ІТ-галузі опублікували відкритий лист щодо запитів СБУ про Інтернет-користувачів. URL: https://ms.detector.media/media_law/law/predstavniki_itgaluzi_opublikuvali_vidkritiy_list_schodo_zapitiv_sbu_pro_internetkoristuvachiv

16. Провайдер не зобов'язаний "зливати" весь трафік спецслужбам. URL: https://ua.112.ua/interview/provaider-ne-zoboviazanyi-zlyvaty-ves-trafik-spetssluzhbam-228237.html

17. Кодекс України про адміністративні правопорушення: Закон України. URL: http://zakon.rada.gov.ua/laws/show/80731-10

18. Carr Madeline Public-private partnerships in national cyber-security strategieshttps. URL: //www.chathamhouse.org/sites/files/chathamhouse/publications/ia/INTA92_1_03_Carr.pdf

19. Про телекомунікації: Закон України. URL: http://zakon.rada.gov.ua/laws/ show/1280-15

20. Are you sharing the same ip address as a criminal? law enforcement call for the end of carrier grade nat (cgn) to increase accountability online. URL: https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end-of-carrier-grade-nat-cgn-to-increase-accountability-online.

21. Про державно-приватне партнерство: Закон України. URL: http://zakon.rada.gov.ua/laws/show/2404-17

22. Положення про Міністерство економічного розвитку і торгівлі України: Постанова Кабінету Міністрів України від 20.08.14 р. № 459. URL: http://zakon.rada.gov.ua/ laws/show/459-2014-%D0%BF

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

УКД 355.402

КРАВЧЕНКО Р.М., *кандидат юридичних наук*

ДІЯЛЬНІСТЬ ВІЙСЬКОВОЇ КОНТРРОЗВІДКИ В АРМІЇ США: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *У статті проведено аналіз організаційно-правових основ (аспектів) діяльності органів військової контррозвідки в армії Сполучених Штатів Америки та вироблено можливі напрямки їх використання у регламентації діяльності військової контррозвідки СБ України.*

Ключові слова: *контррозвідувальне забезпечення, військова контррозвідка, структура, повноваження, розслідування, збройні сили США.*

Summary. *The article analyzes organizational and legal basis (aspects) of the activities of the military counter-intelligence agencies in the United States Army and develops possible directions for their use in the regulation of the military counter-intelligence activities of the Security Service of Ukraine.*

Keywords: *counter-intelligence, military counter-intelligence, structure, powers, investigation, US armed forces.*

Аннотация. *В статье проведен анализ организационно-правовых основ (аспектов) деятельности органов военной контрразведки в армии Соединенных штатов Америки и наработаны возможные направления их использования в регламентации деятельности военной контрразведки СБ Украины.*

Ключевые слова: *контрразведывательное обеспечение, военная контрразведка, структура, полномочия, расследование, вооруженные силы США.*

Постановка проблеми. Інтеграція Збройних Сил України до НАТО висуває певні вимоги щодо проведення процедур управління всією системою оборони країни, у тому числі і її контррозвідувального забезпечення. Вплив права на суспільні відносини, що виникають в армії, має низку особливостей, обумовлених специфікою побудови Збройних Сил, своєрідністю цілей і поставлених перед ними завдань. По-перше, правові норми встановлюють підвищені вимоги до поведінки військовослужбовців у процесі виконання ними обов'язків військової служби. Таке положення визначається характером діяльності армії, складністю і динамічністю збройної боротьби, що вимагає від особового складу високого ступеня організованості й дисципліни. По-друге, норми права більш детально регламентують різні сторони життя і діяльності військовослужбовців. По-третє, право встановлює підвищену відповідальність військовослужбовців за порушення порядку несення військової служби.

Наукове обґрунтування пріоритетів розвитку органів військової контррозвідки Служби безпеки України неможливе без вивчення та упровадження відповідних організаційних та нормативно-правових засад діяльності провідних іноземних спеціальних служб.

Важливість дослідження діяльності військової контррозвідки США зумовлюється багатьма чинниками, зокрема: наявністю в регулятивних нормативних актах цікавих у науковому плані й дієвих на практиці норм та інститутів, які вже були реципійовані спеціальними службами окремих європейських країн; стійкою тенденцією до централізації більшості контррозвідувальних функцій; докладним формулюванням ключових термінів і понять, без яких неможлива ефективна діяльність сучасного контррозвідувального органу.

Результати аналізу наукових публікацій. Елементи функціонування контррозвідувальної системи США з попередження загроз підривного характеру розглядалися І.В. Авдошиним. Окремі аспекти організації контррозвідувальної діяльності іноземних спецслужб були вивчені В.М. Гребенюком. Проблеми законодавчого визначення підстав контррозвідувальної діяльності проаналізовано М.О. Шиліним. О.В. Шмоткіним показано роль спецслужб у реалізації функцій сучасної держави.

Проте спеціальних досліджень нормативно-правового регулювання діяльності органів, що здійснюють контррозвідувальне забезпечення національних військових формувань, не проводилося.

Мета статті полягає в аналізі організаційно-правових засад діяльності військової контррозвідки Армії США та виробленні можливих напрямків їх використання у регламентації діяльності органів військової контррозвідки СБ України.

Виклад основного матеріалу. Американським воєнним експертом Чарльзом Москосом запропоновано три типи взаємозв'язку суспільства та його збройних сил: суспільство готовності до війни, суспільство стримування війни, суспільство відбиття війни. Типу суспільства готовності до війни відповідає за своїми характеристиками більшість країн НАТО та інших воєнних блоків. Внутрішня функція армії зводиться до того, що вона покликана, насамперед, виступати гарантом політичної стабільності суспільства. Зовнішня функція армії полягає в захисті території своєї держави від зовнішніх ворогів, у проведенні політики держави на міжнародній арені із застосуванням збройного насильства [1].

Організаційну структуру Збройних сил США (United States Armed Forces) становить упорядкована сукупність державних організацій**,** озброєних військових формувань**,** установ, закладів тощо Збройних Сил країни, які відповідно до розділу 10 Кодексу США належать до Міністерства оборони США (Армія США, Військово-морські сили, Повітряні сили та Морська піхота) і Міністерства національної безпеки США (Берегова охорона).

До складу Армії США входять понад півмільйона військовослужбовців, переважно з досвідом участі в бойових діях, вони мають сучасне озброєння, а також надійну логістичну систему. Основу сухопутних сил Сполучених Штатів становлять десять бойових дивізій, які підтримуються незначною кількістю бойових бригад. До складу кожної дивізії входять три бронетанкові бригади, механізована піхотна бригада, бригада легкої піхоти, бригада бойових броньованих машин Stryker, повітряно-десантна бригада і повітряно-штурмова бригада, а ще вони доповнені однією авіаційною і однією артилерійською бригадою. До складу дивізії входять від 14000 до 18000 військовослужбовців – залежно від типу кожного окремого підрозділу.

Міністерство армії США (United States Department of the Army) – одне з трьох військових міністерств у системі Міністерства оборони США. Очолює міністерство секретар Армії США, цивільна особа, яка згідно з 10-м розділом Кодексу США відповідає за організаційні та адміністративні питання (не несе відповідальності за застосування армії у військових операціях) в Армії США.

Сучасну систему нормативно-правових актів, що складають правову основу організації і діяльності військової контррозвідки Армії США, можна представити таким чином:

- Конституція США (визначає загальні принципи і закономірності побудови правової основи організації і діяльності контррозвідки);
- федеральні закони США;
- підзаконні нормативні акти;
- акти Президента США (виконавчі накази, директиви, меморандуми тощо);
- акти органів, підпорядкованих Президенту.

Наказом № 381-20 в Армії США введено в дію Контррозвідувальну програму, яка визначає, що Армія здійснює наступальну, комплексну та скоординовану контррозвідувальну діяльність, спрямовану на виявлення, перевірку, оцінку, протидію та припинення іноземної розвідувальної діяльності, саботажу, диверсій, терористичної діяльності та посягань з боку іноземних держав, організацій чи осіб на життя особового складу Армії, військову техніку та бойові спроможності [2].

Згідно з цим наказом, керівництво контррозвідкою Армії здійснює заступник начальника штабу Армії з розвідки, який відповідає за реалізацію Контррозвідувальної програми Армії.

Заступник начальника штабу Армії по роботі з особовим складом забезпечує організацію кадрової роботи, зокрема підбір кандидатів, *виконання випробувальних (термінів) завдань* новопризначеними офіцерами контррозвідки, агентів, помічників та цивільних працівників. Управління навчально-виховної роботи Армії США готує літературу та тренувальні програми, а також впроваджує тренувальні курси для офіцерів та цивільного персоналу, залученого до реалізації Контррозвідувальної програми. Командування Матеріального забезпечення Армії США надає необхідні матеріально-технічні засоби, зокрема обладнання кібербезпеки, а також засоби логістики для здійснення контррозвідувальної діяльності.

Командувач Арміею США, Командувачі Європейським, Тихоокеанським, Південним та іншими Командуваннями здійснюють контррозвідувальні операції та розслідування у сферах своєї відповідальності, під технічним контролем відповідних контрольних відділень. Командувачі Резерву та Національної гвардії проводять відповідну контррозвідувальну діяльність у період мобілізації, а також здійснюють щорічну контррозвідувальну підготовку відповідного персоналу Резерву.

Організацію та координацію контррозвідувальної діяльності в Армії США покладено на Службу розвідки та безпеки Армії США, що:

- проводить тактичну та стратегічну контррозвідувальну діяльність;
- здійснює організацію та управління центральною контрольною системою контррозвідувальної діяльності в Армії США;
- керує роботою Центрального контрольного офісу Армії та контрольних відділень у взаємодії з відповідними Командуваннями Армії, а також створює контрольні відділення в регіонах, де відбувається передове розгортання підрозділів Армії США;
- надає заступнику Начальника Штабу Армії з Розвідки актуальну інформацію про хід та результати контррозвідувальної діяльності;
- сприяє Управлінню навчально-виховної роботи Армії США у розробці концепцій, побудови, тактики і техніки оцінки вразливості з боку засобів технічної розвідки та аналізу безпеки мереж передачі даних;
- передає до Служби кримінальних розслідувань Армії США інформацію, отриману в ході контррозвідувальної діяльності, яка підпадає під юрисдикцію цієї Служби;
- упроваджує автоматизовану інформаційну систему оцінки стану безпеки та програму моніторингу технічної уразливості комп’ютерної безпеки;
- передає до військової поліції та Служби кримінальних розслідувань Армії США інформацію щодо тероризму та інших загроз фізичній безпеці персоналу, отриману в ході контррозвідувальної діяльності. Такі ж відомості передаються до Центру розвідки та аналізу загроз Армії США та Групи антитерористичних операцій та розвідки Армії США.

Для здійснення централізованого управління, контролю, координації та нагляду за контррозвідувальною діяльністю в Армії діє мережа контрольних офісів. Центральному контрольному офісу армії підпорядковуються контрольні відділення.

Центральний контрольний офіс Армії відкриває і припиняє контррозвідувальні розслідування та надає їм контрольні номери, передає їх з одного відділення до іншого, затверджує плани проведення розслідувань, здійснює взаємодію з ФБР та іншими контррозвідувальними структурами.

Організаційною формою діяльності контррозвідки в Армії США є розслідування. Мета контррозвідувального розслідування – забезпечення безпеки персоналу армії, військової інформації, озброєння та техніки, а також встановлення наявності підстав для кримінального переслідування, застосування адміністративних та неюридичних процедур.

Розслідування проводяться за фактами/ознаками або стосовно осіб, причетних до: зради; шпигунства; диверсій; захоплення державної влади; саботажу, ініційованого іноземними розвідувальними службами та службами безпеки; терористичної діяльності, спрямованої проти Армії; вбивств чи завдання тілесних ушкоджень персоналу Армії з боку терористів чи агентів іноземних держав; дезертирства військовослужбовців та втечі цивільного персоналу Армії за кордон, опитування осіб, після повернення на контрольовану США територію; затримання військовослужбовців та службовців Армії іноземними урядовими чи іншими ворожими до США структурами; зникнення або дезертирства військовослужбовців та працівників Армії, які протягом останнього року мали доступ до цілком таємної чи чутливої інформації в сфері оборони, перебували в підрозділах спеціального призначення, мали відношенні до оборонних програм з обмеженим доступом, шифрування; порушення вимог режиму і безпеки, розголошення таємної інформації, несанкціонованого доступу до комп’ютерних систем Армії; вчинення чи спроб вчинення самогубства представниками персоналу Армії, які мали доступ до таємної чи чутливої інформації; неофіційних поїздок військовослужбовців або працівників Армії у визначені країни чи їх контактів з іноземними дипломатами або офіційними іноземними представниками.

Розслідування можуть проводитись щодо таких категорій осіб: військовослужбовців Армії США та членів їх родин; звільнених у відставку військовослужбовців Армії США, якщо обставини, які розслідуються, мали місце в період дійсної служби; військовослужбовців та резервістів Резерву Армії США, якщо обставини, які розслідуються, мали місце в період дійсної служби; найманих працівників американської Армії, включаючи іноземний персонал та членів їх сімей; іноземних громадян, які звернулися з питань працевлаштування в Армії; діючих та звільнених військовослужбовців і працівників Міністерства оборони США.

На підрозділи військової контррозвідки покладено обов’язки із проведення радіоконтррозвідувальних заходів, до яких належать:

- систематична перевірка випромінювання електронних засобів зв’язку для визначення їх уразливості з боку ворожих систем перехоплення сигналів;

- розвиток і підтримання в актуальному стані деталізованої бази даних засобів електронного перехоплення та цілевизначення, які використовуються іноземними розвідувальними службами;

- збір та аналіз даних про провідні та мобільні мережі передачі даних, особливо важливі вузли електрозв’язку, які безпосередньо використовуються в інтересах розвідки та управління військами, а також систем, які здійснюють випромінювання, що може дозволити іноземним розвідувальним структурам виявляти, відстежувати та визначати місцезнаходження військових підрозділів та об’єктів;

- відстеження сигналів власного телекомунікаційного обладнання для встановлення рівня безпеки кодів та криптографічної апаратури;

- оцінювання категорій і цінності інформації, витік якої може відбутися внаслідок перехоплення іноземними технічними розвідками;

- визначення ефективності електронного захисту та протидії.

Армійські командири всіх рівнів зобов'язані негайно надавати до відповідних підрозділів контррозвідки Армії інформацію, яка стала їм відома і становить чи може становити контррозвідувальний інтерес. Водночас підрозділи контррозвідки Армії при отриманні первинної вагомої для захисту збройних сил інформації повинні негайно передавати її командирам відповідних рівнів.

Якщо підрозділ контррозвідки Армії випадково отримує інформацію про міжнародний трафік наркотичних речовин, вона повинна бути протягом 5 днів передана до Управління по боротьбі з наркотиками США.

Важливим джерелом отримання контррозвідувальної інформації є опитування перебіжчиків і американських полонених, які можуть володіти відомостями щодо особистостей, форм і методів, організації діяльності іноземних розвідувальних служб, терористичних організацій та політичних екстремістів, перебіжчиків, що мали доступ до таємної інформації, здійснювали співробітництво з іноземними розвідками в період чи після дезертирства. Опитування перебіжчиків та полонених зазвичай проводиться армійськими дізнавачами у взаємодії з військовими контррозвідкниками на підставі положень Директиви Армії США № 34-52 [3].

Одна з функцій Армії США – контррозвідувальний аналіз, який передбачає прогнозування розвідувальної обізнаності противника та можливі варіанти прийняття командних рішень на основі отриманої розвідінформації, а також сприяння у дезінформуванні противника щодо оперативних планів командування, заходів із захисту інформації в телекомунікаційних мережах. Стратегічний контррозвідувальний аналіз передбачає узагальнення результатів контррозвідувального аналізу тактичного рівня в інтересах надання допомоги у прийнятті рішень армійським командуванням.

Об'єктом контррозвідувального аналізу є три види іноземної розвідувальної діяльності: агентурна, радіоелектронна та видова розвідка.

Протидія кожному з цих розвідувальних проявів передбачає проведення контррозвідувального аналізу, який включає: оцінку загроз від агентурної, радіоелектроної та видової (включаючи польову, повітряну та космічну) розвідок, а також підривних дій (тероризму, диверсій, антидержавної діяльності та саботажу); оцінку уразливості особового складу, військової техніки, радіоелектронних засобів та планів застосування бойових підрозділів від вказаних видів розвідувальної та підривної діяльності; прогноз можливого негативного впливу розвідувальної та підривної діяльності на виконання завдань військовим формуванням; розробку заходів протидії, у тому числі визначення цілей для взяття під оперативний чи технічний контроль, нейтралізацію чи знищення; упровадження заходів протидії; оцінку ефективності вжитих заходів протидії.

Співробітники військової контррозвідки не можуть залучатися до розслідування військових злочинів, кримінальних вчинків проти цивільного населення чи їхнього майна, інших злочинних дій, що не підпадають під юрисдикцію контррозвідки. На відміну від Служби кримінальних розслідувань Армії США, контррозвідка армії здійснює кримінальне переслідування тільки у випадках посягань на національну безпеку.

Військовослужбовці, які виконують контррозвідувальні функції, представляються як "спеціальний агент контррозвідки Армії США" та "помічник спеціального агента контррозвідки Армії США". Спеціальні агенти та їх помічники в межах проведення контррозвідувального розслідування чи операції мають право доступу до архівів та документів Армії США до вищого грифа секретності включно, уповноважені робити їх

копії чи виписки. Також офіцери військової контррозвідки мають право відвідувати всі території та приміщення Армії США з дотриманням відповідних вимог безпеки.

Директива Армії США № 195-6 регламентує здійснення досліджень із використанням поліграфа за наявності наступних підстав [4]: перевірка цивільних працівників, військовослужбовців, співробітників фірм-контракторів у зв'язку з проведенням контррозвідувального розслідування; перевірка придатності, надійності та правдивості агентів, залучених до контррозвідувальних операцій; перевірка осіб у зв'язку з наданням доступу до інформації з обмеженим доступом чи робіт, призначенням до розвідувальних підрозділів Армії чи Міністерства оборони, доступом до шифрувальних документів та приміщень.

Бойовий статут Армії США № 34-60 "Контррозвідка" визначає, що контррозвідувальне забезпечення Армії в першу чергу полягає у наданні командирам всіх рівнів чіткої інформації про наявні загрози іноземної розвідувальної діяльності та рекомендацій із захисту від них [5]. Контррозвідувальна діяльність, крім проведення розслідувань, включає здійснення наступальних та оборонних операцій, аналіз уразливості та стану безпеки, збір розвідувальної інформації в мирний та воєнний час для задоволення потреб військового командування. Роль контррозвідки полягає в підтримці діяльності командування із забезпечення необхідного рівня секретності та прямому чи опосередкованому захисті сил.

Контррозвідувальна діяльність в Армії покладається не тільки на агентів та технічних фахівців контррозвідки, обов'язком всього особового складу Армії є виконання належних заходів безпеки, спрямованих на мінімізацію іноземної розвідувальної діяльності.

До виконання завдань з протидії іноземній розвідувальній діяльності можуть залучатися розвідувальні підрозділи, військова поліція, цивільні установи та органи влади, бойові та підрозділи військово-цивільного співробітництва і психологічних операцій, підрозділи кримінальних розслідувань.

Директивою Міністерства оборони США № 5240.6 встановлено, що для персоналу військового відомства проводяться періодичні брифінги щодо загроз іноземної розвідувальної діяльності, міжнародного тероризму, втручання в комп'ютери та мережі, розголошення інформації з обмеженим доступом, а також обов'язків співробітників повідомляти про вказані факти та ознаки [6].

Згідно з Директивою Армії США № 381-12 "Розвідувально-підривна діяльність проти Армії США", особовий склад повинен не менше одного разу на рік проходити інструктажі з наступних питань [7]: доведення інформації про те, що іноземні розвідувальні служби вважають особовий склад Армії США цінним джерелом таємної та чутливої нетаємної оборонної інформації; характеристика кримінального покарання за шпигунство та інші злочини проти національної безпеки; роз'яснення форм і методів діяльності іноземних розвідок, способів потрапляння в залежність від них, залучення до агентурної діяльності під "чужим прапором"; наведення ознак шпигунства і ситуацій, про які необхідно доповідати; характеристика загроз міжнародного та внутрішнього тероризму та превентивних заходів, які повинні застосовуватися особовим складом та членами сімей [8].

Для певних категорій військовослужбовців (тих, що мають доступ до особливо важливої таємної інформації, криптографічних даних, науково-технічної діяльності оборонної спрямованості, розвідувальної діяльності, планують виїхати до визначених країн, взяти участь у міжнародних науково-технічних заходах, верифікаційній діяльності, виконувати обов'язки військових аташе за кордоном) офіцерами контррозвідки проводяться індивідуальні інструктажі.

Представники особового складу Армії США повинні доповідати до підрозділів військової контррозвідки про: спроби неуповноважених осіб отримати таємну чи нетаємну

інформацію щодо спроможностей, персоналу, діяльності, технологій Армії США шляхом опитування, вивідування, введення в оману, підкупу, погроз, шантажування, фотографування, спостереження, збирання документів чи матеріалів, проникнення до комп'ютерів; відомі чи підозрювані факти шпигунської діяльності з боку персоналу Армії США; контакти персоналу Армії США або членів їх родин з особами, підозрюваними у причетності до іноземних розвідок, служб безпеки чи терористичних організацій; контакти персоналу Армії США з офіційними представниками чи іншими громадянами іноземних держав, якщо вони проявляють підвищену поінформованість або необґрунтований інтерес до представників Армії США чи їх обов'язків чи проявляють необґрунтований інтерес до американських технологій, досліджень, систем озброєння чи наукової інформації.

Директива № 381-12 встановлює, що військовослужбовці Армії США також повинні доповідати до підрозділів військової контррозвідки іншу інформацію, яка може становити контррозвідувальний інтерес:

- виявлення в приміщеннях, що входять до зон безпеки, зокрема конференц-залах, підозрілих прослуховуючих пристроїв чи інших засобів технічного спостереження. Також поводження із вказаними пристроями визначається Директивою Армії США № 381-14 (S) [9];
- несанкціонована або незрозуміла відсутність представників персоналу Армії США, які мали доступ до цілком таємної інформації, криптографічних даних, входять до складу підрозділів спеціального призначення;
- самогубства чи спроби покінчити з життям з боку військовослужбовців, які протягом попереднього року мали доступ до таємної інформації;
- порушення заходів комп'ютерної безпеки;
- вбивства чи замахи на життя з боку членів терористичних організацій чи агентів іноземних спецслужб;
- втеча чи спроба втечі до іноземної держави військовослужбовця Армії США;
- затримання військовослужбовця Армії США органом влади іноземної держави;
- незаконне використання особою документів, що вказують на приналежність до розвідки Армії США;
- розкриття особи співробітника американської розвідки, залученого до таємної розвідувальної чи контррозвідувальної діяльності;
- пропонування іноземною державою працевлаштування для громадянина США в сфері розробки, виробництва, використання ядерної зброї.

Доповіді в підрозділи військової контррозвідки також підлягає наступна інформація щодо ознак шпигунства: будь-які спроби отримати розширений доступ до таємної інформації особою, яка намагається терміново влаштуватися на службу, або виконувати роботи, що перевищують обсяги, встановлені функціональними обов'язками чи понад робочий час; несанкціоноване переміщення таємних матеріалів з робочого місця, їх перебування в особистому транспорті чи за місцем мешкання особи; використання копіювальної, факсимільної та комп'ютерної техніки для розмноження таємних документів, що не викликано службовою необхідністю; перебування особи в приміщенні, де обробляється чи обговорюється таємна інформація, маючи при собі недозволені засоби реєстрації чи передачі інформації; невмотивовані прибутки; часті і невмотивовані короткочасні виїзди до іноземних країн; намагання запропонувати особі, допущеній до чутливої інформації, додаткового прибутку від сторонніх підприємств, чи її втягування в кримінальну ситуацію, що створює передумови для шантажу; відвідування іноземних посольств, консульських установ, торгівельних чи прес-офісів.

Представники особового складу Армії США, які володіють інформацією про факти та ознаки розвідувально-підривної діяльності, повинні негайно доповідати про зазначене до найближчого підрозділу військової контррозвідки, а якщо це не представляється можливим, то власному військовому командуванню, яке в подальшому, але не пізніше як протягом 24 годин, повинно скерувати отримані дані до військової контррозвідки. Якщо вказана інформація була отримана під час перебування за кордоном, вона повинна доповідатися після повернення до США, а в невідкладних випадках представникам військового командування, офіцерам розвідки чи безпеки, військовим аташе чи до консульської установи.

У випадку отримання інформації про порушення заходів безпеки, випадки тероризму чи втручання в комп'ютерні мережі, військовослужбовці повинні діяти згідно з Директивою Армії США № 380-5 [10], 525-13 [11] та 380-19 [12] відповідно.

Висновки.

Контррозвідувальна діяльність визначена як первинна функція Армії по захисту власного особового складу, інформації та бойової техніки, у зв'язку з чим відомчими нормативними актами встановлені завдання і права військових контррозвідників та обов'язки персоналу Армії у сфері контррозвідувального пошуку, перевірки, проведення операцій та режиму.

Компетенція військової контррозвідки поширюється на протидію розвідувальній і підривній діяльності іноземних спецслужб і терористичних організацій, державній зраді, антидержавним проявам, забезпечення охорони інформації з обмеженим доступом, комп'ютерної інформації та мереж передачі даних. Залучення співробітників військової контррозвідки до протидії іншим протиправним проявам або виконання завдань, не пов'язаних з контррозвідувальною діяльністю, заборонено.

Встановлено вичерпний перелік фактів та ознак, за якими проводяться контррозвідувальні розслідування, категорій осіб, що можуть бути їх об'єктами, здійснено розмежування функцій військової контррозвідки з іншими розвідувальними, правоохоронними та спеціальними органами. Також визначені об'єкти, завдання та мету контррозвідувального аналізу, якою є надання командирам відповідних рівнів інформації про наявні загрози іноземної розвідувальної діяльності та рекомендацій із захисту від них.

Військовослужбовці Армії США зобов'язані проходити опитування з боку військової контррозвідки в зв'язку з перебуванням в підозрілих ситуаціях (полон, перебування на ворожій території та ін.). Військові посадові особи та представники органів влади зобов'язані передавати до підрозділів військової контррозвідки отриману ними інформацію в сфері компетенції останніх, а також надавати сприяння та брати участь у контррозвідувальних заходах. Уповноважені представники військової контррозвідки мають право, в межах виконання своїх обов'язків, здійснювати доступ до всіх документів та приміщень Армії США.

Підрозділи військової контррозвідки перебувають на всіх видах забезпечення Армії США.

Використана література

1. Charles C. Moskos From Institution to Occupation. Trends in Military Organization. URL: http://journals.sagepub.com/doi/10.1177/0095327X7700400103

2. The Army Counterintelligence Program. URL: https://fas.org/irp/doddir/army/ar381-20.pdf

3. FM 34-52. Intelligence Interrogation. URL: https://fas.org/irp/doddir/army/fm34-52.pdf

4. Department of the Army Polygraph Activities – Army Publishing. URL: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwid5o6X3-AhUwxaYKHVsMCAsQFjAAegQIARAC&url=https%3A%2F%2Farmypubs.army.mil%2Fepubs%2FDR_pubs%2FDR_a%2Fpdf%2Fweb%2FAR195-6_Web_FINAL.pdf&usg=AOvVaw1f2gih3WuiqVZF656ah3_2

5. FM 34-60. Counterintelligence. URL: https://www.aclu.org/files/projects/foiasearch/pdf/DODDOA006278.pdf6

6. Department of Defense INSTRUCTION. URL: https://fas.org/irp/doddir/dod/i5240_6.pdf

7. Threat Awareness and Reporting Program. URL: https://fas.org/irp/doddir/army/ar381-12.pdf

8. UNIFORM CODE OF MILITARY JUSTICE. Congressional Code of Military Criminal Law applicable to all military members worldwide. Use the links below for a quick tour of the UCMJ. URL: http://www.au.af.mil/au/awc/awcgate/ucmj.htm

9. SECRET. Army regulation. URL: http://hourofthetime.com/1-LF/AR381-14c.pdf

10. SAFEGUARDING MILITARY INFORMATION. URL: https://www.nsa.gov/news-featu res/declassified-documents/friedman-documents/assets/files/reports-research/FOLDER_057/41699469073880.pdf

11. A Leader’s Handbook to Unconventional Warfare. URL: https://info.Publicintelligence.net/USArmy-LeadersUW.pdf

12. AR 380-19. Information Systems Security. URL: https://fas.org/irp/doddir/army/ar380-19/toc.htm

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

УДК 343.985:343.326

КВАСЮК В.В., аспірант Національної академії СБУ

ОСНОВНІ ПІДХОДИ ДО ВИЗНАЧЕННЯ ПОНЯТТЯ “БІОТЕРОРИЗМ”

Анотація. *У статті висвітлюються загальні підходи до визначення поняття “біотероризм”, з’ясовується сутність та особливості біотероризму як виду технологічного тероризму. Акцентується увага на чинниках, що зумовлюють підвищену суспільну небезпеку проявів біотероризму .*

Ключові слова: *технологічний тероризм, біотероризм, біологічні агенти, біологічна зброя, біологічна безпека.*

Summary. *The article highlights the general approaches to the definition of the term “bioterrorism”, defines the essence and features of bioterrorism as a special type of technological terrorism. Attention is focused on the factors causing an increased risk of manifestations of bioterrorism.*

Keuwords: *technological terrorism, bioterrorism, biological agents, biological weapons, biological security.*

Аннотация. *В статье освещены общие подходы к определению понятия “биотерроризм”, определяется сущность и особенности биотерроризма как особого вида технологического терроризма. Акцентируется внимание на факторах, обуславливающих повышенную опасность проявлений биотерроризма.*

Ключевые слова: *технологический терроризм, биотерроризм, биологические агенты, биологическое оружие, биологическая безопасность.*

Постановка проблеми. Тероризм є однією з найбільш серйозних загроз міжнародному миру і безпеці людства. У Концепції боротьби з тероризмом, затвердженої Указом Президента України від 25.04.2013 року № 230, зазначається, що подальше поширення терористичної загрози обумовлюється процесами світової глобалізації, інтернаціоналізації, що тривають [1]. Слід зауважити, що глобалізація, з одного боку, має свої переваги, з іншого – поєднана із серйозними ризиками, оскільки імпорт продуктів харчування з інших країн створює додаткові можливості застосування засобів біотероризму для терористів.

Звісно, виникнення біотероризму пов’язується з стрімким розвитком генної інженерії та появою новітніх біотехнологій, що значно ускладнює проблему протидії цьому небезпечному явищу. Сьогодні терористи для досягнення своїх протиправних цілей обирають асиметричні методи ведення війни, зокрема, хімічну та біологічну зброю.

На думку фахівців, біологічна зброя є найбільш небезпечною серед засобів масового знищення, оскільки має найвищий порівняно з іншими видами зброї, вражаючий потенціал. Застосування останньої, безперечно, може призвести до катастрофічних наслідків, зважаючи на те, що біологічна зброя є надзвичайно мобільною та володіє високою вражаючою здатністю [2, с. 18]. Щоб реалізувати свої цілі, терористи не зупиняються й перед використанням біологічних агентів з різним потенціалом патогенності. Терористичні групи та організації, які здатні використовувати біологічні агенти як інструмент тероризму, розрізняються за складом, етнічною належністю, джерелами фінансування, ідеологією, мотивацією. Серед них виділяються великі, добре фінансовані організації, опозиційні повстанські групи і політичні рухи, релігійні

і культові секти, що пропагують ідеологію “кінця світу”, різного роду націоналістичні групи, а також терористи-одинаки. Застосування терористами різних видів біологічної зброї може викликати епідемію, здатну спричинити загибель величезної кількості людей, тварин і сільськогосподарських культур.

Іноді метою терористів є вибіркове ураження окремих громадських чи державних діячів або спричинення якомога більшої кількості жертв серед цивільного населення для залякування людей.

Потреба чіткого визначення поняття “біотероризм” виникає у зв’язку з необхідністю узгодження досліджень цього явища, координації дій суб’єктів боротьби з тероризмом як на національному, так і міжнародному рівнях.

Результати аналізу наукових публікацій. Окремі аспекти біотероризму досліджувалися у працях М.Т. Васильєва, М.В. Гребенюка, О.О. Головацького, Б.Д. Леонова, Р.О. Мартинюка, Г.Г. Онищенко, Д.Л. Поклонського, Р.І. Сибірної, М.Ю. Тарасова, В.В. Татаринова та інших вчених. Разом з тим, дедалі більшої уваги потребують поглиблені наукові дослідження біотероризму в контексті визначення його суті та ознак.

Метою статті є визначення біотероризму з урахуванням основних підходів, що склалися у юридичній науці.

Виклад основного матеріалу. На рубежі століть біологічний тероризм як прояв технологічного тероризму починає відігравати домінуючу роль серед загроз міжнародній безпеці. Відповідно до ст. 1 Закону України “Про боротьбу з тероризмом” під технологічним тероризмом слід розуміти злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров’я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру [3].

Стаття 1 Конвенції ООН про заборону розробки, виробництва та накопичення запасів бактеріологічної (біологічної) і токсинної зброї та про їх знищення від 10 квітня 1972 року забороняє державам-учасникам розробляти, виробляти, накопичувати, отримувати і зберігати: (1) біологічні агенти або токсини таких видів та у такій кількості, що не передбачені для профілактичних, захисних чи інших мирних цілей; (2) зброю, обладнання або засоби доставки, призначені для використання таких агентів або токсинів у ворожих цілях чи у збройних конфліктах [4].

Вікіпедія визначає біотероризм як тип тероризму, що супроводжується розповсюдженням біологічних агентів, тобто бактерій, вірусів або токсинів, так само як і методів їхньої доставки, як в природній, так і в модифікованій людиною формі, тобто з використанням біологічної зброї [5].

На думку Гребенюка М.В. та Леонова Б.Д., біотероризм як особливо небезпечний різновид тероризму являє собою використання біологічних агентів, бактерій або токсинів для масштабного знищення продовольчих, біологічних ресурсів будь-якої країни з метою встановлення зовнішнього тотального контролю над ними, підриву продовольчої незалежності [6, с. 90].

На думку американського дослідника В. Каруса, біотероризмом є особлива форма тероризму, пов’язана з умисним екологічним викидом патогенів (вірусів, бактерій, паразитів, грибів, токсинів), які викликають хворобу чи смерть людей, тварин чи рослин.

Поширення відбувається шляхом вивільнення аерозолів як доповнення до вибухових речовин або шляхом отруєння продуктів чи водних ресурсів [7].

Дослідження свідчать про те, що деякі патогени являють собою значну загрозу для національної безпеки, особливо в АПК, де характерним є використання біологічної та токсинної зброї з метою руйнування культур, рослин, тварин, інших видів життя, їжі, води, інших предметів продовольчого забезпечення, які використовуються для підтримки сільського господарства та продовольчої системи держави з метою залякування населення, дестабілізації політичної ситуації в країні.

З точки зору О.О. Головацького, біотероризм відрізняється від інших видів тероризму тим, що його деструктивний потенціал пов'язаний з ураженням живої сили, тобто людей, без заподіяння шкоди матеріальним об'єктам. Для досягнення своєї мети терористи використовують різні методи, але особливу небезпеку для людства являє собою загроза несподіваного використання зброї масового знищення – хімічної, бактеріологічної, радіологічної, ядерної. Проте особливістю біологічної зброї є те, що її надзвичайно складно виявити, а ефект від її застосування може бути відкладеним та прихованим на значний термін, що збільшує кількість її потенційних жертв [2, с. 18].

Зокрема, патогени (біологічні агенти, або мікроби) фактично складно виявити, і вони відносно легко можуть бути як ввезені у будь-яку країну світу, так розмножені у великій кількості. Головними групами або класами патогенів, які можуть викликати інфекційні хвороби, є:

1) бактерії, які можуть викликати такі хвороби, як сибірська виразка, чума і туляремія. Хоча багато патогенних бактерій чутливі до антибіотиків, деякі їх штами стійкі до них і здатні існувати в природних умовах;

2) віруси, що викликають хвороби і можуть виникати в живих тканинах;

3) рикетсії, прикладом яких є бактерії, що викликають лихоманку;

4) гриби, деякі з яких можуть бути використані проти людини, але найбільш небезпечні для сільськогосподарських культур;

5) токсини, тобто продукти життєдіяльності мікроорганізмів (токсин ботулізму або ентеротоксин У стафілокока), рослини (рицин з бобів рицини) або молюскі (сакситоксин) [5].

Спектр збудників, які можливо використати з біотерористичною метою, по суті такий самий, як і спектр інфекцій, що становлять загрозу для будь-якої країни у разі ввезення з-за її меж, або збудників, що циркулюють у державі (у природних чи інших вогнищах) [8, с. 498].

Крім цього, висока небезпека проявів біотероризму зумовлюється наступними чинниками:

1) доступністю біологічної зброї, так як мікроорганізми, які можуть бути використані як агенти, існують у природі;

2) не достатньою вивченістю вірусів і мікроорганізмів. Крім того, в природніх умовах постійно виникають нові патогени – так звані "виникаючі інфекції". Тільки за 20 років зареєстровано більше 30 нових інфекційних агентів, таких як віруси Марбург, Ебола, проти яких дотепер немає достатніх засобів лікування і профілактики;

3) простотою виготовлення біологічної зброї. Сьогодні у світі 22 тис. лабораторій, здатних виробляти біологічну зброю [2, с. 18].

4) зручністю зберігання і транспортування біологічної зброї;

5) складністю виявлення біологічних агентів, у порівнянні з хімічними і радіологічними;

6) широким розповсюдженням при використанні біологічної зброї вражаючого агента, складністю виявлення місця застосування цієї зброї і неможливістю обмеження зони теракту;

7) потреба великій кількості вакцин та/або антибіотиків для надання допомоги постраждалим [9, с. 36].

Найбільш доступними і небезпечними засобами біотероризму на сьогодні є патогени сибірської виразки, натуральної віспи, геморагічної лихоманки і рицини, хоча ряд обставин ускладнюють їх використання для великомасштабних терактів. Найбільш відомим випадком біотероризму вважається розповсюдження листів зі збудниками сибірської виразки у вересні-жовтні 2001 року у США, внаслідок якої померло 5 осіб, більше 20 було інфіковано, декілька тисяч осіб були змушені вживати антибіотики [10, с. 5]. Можна також згадати спалах екзотичної хвороби Ньюкасла серед домашньої птиці в США, викликаний контрабандою птахів з Мексики. Захворюваність привела до значних збитків, оскільки витрати на ліквідацію склали приблизно 168 млн. дол. США. Один з патогенів викликає ящур (FMD) – небезпечний вірус, здатний поширюватися на 170 миль, досягаючи 23 станів через п’ять днів. Орієнтовні втрати від спалаху ящура за один тиждень складали близько 447,76 млн. дол. США. Наприклад, в Бельгії фермери оцінили втрати у 812 мільйонів євро за перші два тижні спалаху ящура. Тайвань втратив 4 мільярди доларів, падіння цін на свиней досягало 60 %, 50 тисяч працівників втратили роботу, а міжнародне ембарго було оцінено у 15 мільярдів доларів США [11].

Викладене свідчить про те, що спільне розуміння феномену біотероризму потрібне також для отримання надійних статистичних даних про масштаби цього суспільно небезпечного явища.

Висновки.

На нашу думку, біотероризм є особливим різновидом технологічного тероризму, для якого характерним є використання біологічної та токсинної зброї з терористичною метою шляхом отруєння атмосфери, водних ресурсів, продуктів харчування чи інших предметів продовольчого забезпечення або знищення чи руйнування рослинного або тваринного світу.

Перспективи подальших досліджень є визначення концептуальних, правових та організаційних засад системи протидії біотероризму в Україні.

Використана література

1. Концепція боротьби з тероризмом: Указ Президента України від 25.04.13 р. № 230. *Офіційний вісник України*. 2013. № 34. Ст. 1202.

2. Головацький О.О. Біотероризм: особливості та тактика протидії. *Південноукраїнський правничий правопис*. 2016. № 1. С. 18-20.

3. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180.

4. Про заборону розробки, виробництва та накопичення запасів бактеріологічної (біологічної) і токсинної зброї та про їх знищення: Конвенція ООН від 10 квітня 1972 року. URL: http://zakon.rada.gov.ua/laws/show/995_054 (назва з екрана, дата звернення: 20.09.2018).

5. Біотероризм. URL: https://uk.wikipedia.org/wiki/%D0%91%D1%96%D0% BE%D1%82% D0%B5%D1%80%D0%BE%D1%80%D0%B8%D0%B7%D0%BC (назва з екрана. дата звернення: 20.09.2018).

6. Гребенюк М.В. Леонов Б.Д. Інформаційна складова запобігання проявам аграрного тероризму. *Правова інформатика*. № 2/2014. С. 90-94.

7. Carus W.S. The Threat of Bioterrorism. National Defense University, Institute for National Strategic Studies, Washington, D.C. URL: http://www.au.af.mil/au/awc/awcgate/ndu/forum 127.htm (назва з екрана, дата звернення: 20.09.2018).

8. Сибірна Р.І., Сибірний А.В. Проблеми боротьби із загрозою біотероризму в Україні. *Вісник Національного університету "Львівська політехніка"*. 2016. С. 495-499.

9. Курзова В.В. Актуальні питання правового регулювання міжнародного співробітництва України в сфері боротьби з тероризмом. *Митна справа*. 2013. № 6. С. 34-43.

10. Васильев Н.Т., Тарасов М.Ю., Поклонский Д.Л. Биологический терроризм: прошлое, настоящее, будущее. *Химическая и биологическая безопасность*. Київ: Винити, 2002. Вип. 6. С. 3-10.

11. Agroterrorism: Risks, Threats, and Teamwork URL: https://www.researchgate.net/publication/305493040_Agroterrorism_Risks_Threats_and_Teamwork (назва з екрана, дата звернення: 20.09.2018).

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

УДК 340+681.3

ВЕРГОЛЯС О.О., аспірант НДІІП НАПрН України

ІНФОРМАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ СПЕЦІАЛЬНИХ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ

Анотація. *В цій статті проаналізовано роль та місце інформаційного етапу спеціальних інформаційних операцій (на прикладі операції "Гюльчатай" центру "Миротворець") у загальному алгоритмі проведення спеціальних інформаційних операцій, а також розглянуто актуальний стан та проблеми правової регламентації спеціальних інформаційних операцій на сучасному етапі.*

Ключові слова*: інформаційні операції, спеціальні інформаційні операції, інформаційні війни, інформаційний привід, стратегічні комунікації.*

Summary. *This article analyzes the role and place of the information phase of the special information operations (on the example of Operation "Gulchatay" of the "Peacemaker" Center) in the general algorithm for carrying out special information operations, as well as the current state and problems of legal regulation of special information operations at the present stage.*

Keywords: *information operations, special information operations, information wars, information retrieval, strategic communications.*

Аннотация. *В этой статье проанализированы роль и место информационного этапа специальных информационных операций (на примере операции "Гюльчатай" центра "Миротворец") в общем алгоритме проведения специальных информационных операций, а также рассмотрены актуальное состояние и проблемы правовой регламентации специальных информационных операций на современном этапе.*

Ключевые слова: *информационные операции, специальные информационные операции, информационные войны, информационный повод, стратегические коммуникации.*

Постановка проблеми. Поняття "ноосфери", запропоноване французьким ученим Едуардом Леруа та розвинене його сучасниками Пьером Тейяр де Шарденом та В.І. Вернадським, наприкінці минулого століття набуло нового значення. У 1990-х роках експерти аналітичного центру RAND адміністрації США Дж. Аркилла та Д. Ронфельд запропонували об'єднати існуючі поняття кіберпростору й інформаційної сфери як сукупності кіберпростору й засобів масової інформації в єдину "ноосферу", засновану на ідеях, духовних цінностях, етиці епістемологічну парадигму, у якій на зміну традиційній політиці "грубої" сили з її акцентом на матеріальну складову протиборства приходить нова, заснована на "м'якій силі", так звана "ноовійна", війна інформаційна [1]. Інформаційна війна являє собою різновид бойових дій, зброєю в яких виступають обладнання й методи обробки інформації, що дозволяють цілеспрямовано, швидко й потай впливати на військові й цивільні інформаційні системи супротивника з метою підриву його політики, економіки, боєздатності, в остаточному підсумку – національної безпеки. [2, с. 204, 108-109].

Концепція інформаційної війни передбачає проведення інформаційних операцій – комплексу взаємозалежних за метою, місцем і часом заходів і акцій, спрямованих на ініціалізацію й управління процесами маніпулювання інформацією, з метою досягнення й утримання інформаційної переваги шляхом впливу на інформаційні процеси в інформаційних системах супротивника [3, с. 191-193].

На сьогоднішній день жодними нормативно-правовими актами України не врегульований та не закріплений алгоритм проведення спеціальних інформаційних операцій (далі – СІО), що відбивається на ефективності й результативності зазначених заходів. Прогалина у законодавстві частково компенсується сталою практикою владних структур, на які покладені функції з проведення СІО, що, однак, повністю не вирішує питання проведення ефективних операцій з вигідного впливу на цільову аудиторію СІО.

Вдосконаленню нормативно-правової бази, яка регулює діяльність вітчизняних спецслужб та правоохоронних органів в частині правової регламентації проведення СІО може сприяти належне теоретичне підґрунтя, зокрема, розроблений науковцями загальний алгоритм проведення СІО [4], оптимізації якого, у свою чергу, має сприяти комплексне дослідження інформаційного етапу СІО, яке має на меті збільшити ефективність як інформаційно-психологічного впливу на цільову аудиторію, так і оптимізувати використання людських та матеріально-технічних ресурсів в ході проведення СІО.

Результати аналізу наукових публікацій. Питання організації та планування СІО при забезпеченні національної безпеки та у правоохоронній діяльності розглядались такими вченими як Богданова Ю., Голубев С., Гриняев С., Зуева Н., Иванов И., Козирацкий Ю., Кушнір О., Ланде Д., Ліпкан В., Лизанчук В., Литвиненко О., Макаренко С., Панченко В., Прохоров Д., Резепов И., Чадов И., Черных С., Фурашев В.

У той же час слід констатувати, що наразі залишаються недостатньо вивченими проблеми, пов’язані із дослідженням інформаційно-правового забезпечення СІО.

Метою статті є визначення ролі та місця інформаційного етапу СІО у загальному алгоритмі проведення СІО, а також актуального стану правової регламентації проведення СІО на сучасному етапі, вироблення на цій основі певних рекомендацій щодо вдосконалення інформаційно-правового забезпечення СІО.

Виклад основного матеріалу. Розпочинаючи дослідження проблематики СІО, передусім слід визначитись з категорією більш загального порядку – інформаційними операціями, котрі є складовою інформаційної війни. Під інформаційними операціями традиційно розуміють дії, що застосовуються для досягнення інформаційних переваг у забезпеченні воєнної стратегії шляхом впливу на інформацію, інформаційні системи та інформаційну інфраструктуру супротивника з одночасним посиленням забезпечення безпеки власної інформації, інформаційних систем та інформаційної інфраструктури [5].

У сучасних умовах не викликає сумніву також і той факт, що інформаційні операції можуть проводитись не лише у воєнній, але й в інших сферах забезпечення національної безпеки, зокрема, у правоохоронній, що додатково підсилює роль та значення інформаційних операцій в умовах ведення гібридної війни.

За характером завдань, які вирішують інформаційні операції, вони класифікуються на оборонні і наступальні. Метою оборонних інформаційних операцій – забезпечення виконання цільових завдань інформаційними й керуючими системами в умовах ведення інформаційної війни, а також забезпечення схоронності інформаційних ресурсів і запобігання витоку, викривлення, втрати або викрадення інформації в результаті несанкціонованого доступу до неї з боку супротивника. Метою наступальних інформаційних операцій є досягнення й утримання інформаційної переваги в інформаційній війні. Наступальні інформаційні операції являють собою комплексне проведення за єдиним задумом і планом заходів щодо оперативного маскування, радіоелектронної боротьби, програмно-математичного впливу на інформаційно-керовані системи, фізичного знищення (або виведення з ладу) об’єктів інформаційної інфраструктури. У ході таких операцій здійснюються заходи, що передбачають вплив на

свідомість людей і спрямовані на зрив процесу прийняття рішень, а також дії з метою порушення роботи або знищення елементів інформаційної інфраструктури [2; 6 – 7].

У ході інформаційних операцій використовуються різні прийоми протиборства: одержання інформації про супротивника як у результаті аналізу відкритої інформації, що циркулює в ЗМІ, інформаційних системах тощо, так і в результаті її перехоплення, несанкціонованого доступу з наступним викривленням, знищенням, "перекодуванням" з метою формування оцінки, наміру й орієнтацій населення й осіб, що ухвалюють стратегічні рішення; придушення елементів інфраструктури державного й військового управління; радіоелектронна боротьба тощо. Методи інформаційної війни надзвичайно різноманітні: дезінформація, пропаганда, наклеп, неправда, приховування істотної інформації, зсув понять, відволікання уваги, інформаційне табуювання й інші.

Фахівці також визначають інформаційні операції як сукупність заходів гласного та негласного характеру, спрямованих на приховане керування процесами інформаційної сфери. На відміну від пропагандистських заходів, вони мають обмежену у часі тривалість, підпорядковані конкретній меті та координуються єдиним центром – спеціальними службами [4]. Зокрема, як інформаційні операції в ході гібридної війни РФ проти України В. Панченко характеризує події навколо обстрілу блокпоста під Слов'янськом, після якого вщент згоріло все майно, але залишились неспаленими паперові візитівки лідера Правого сектору Д. Яроша, а також фішингову атаку на сайт ЦВК України під час виборів Президента України у травні 2014 року, коли відображені на ньому результати голосування свідчили про перемогу знову ж таки Д. Яроша [8, с. 14-15]. Фактично в даному випадку мова йде про СІО.

Отже, СІО – це інформаційні операції, які проводяться в інтересах забезпечення національної безпеки з використанням сил безпеки і оборони [9] (у даному випадку вважаємо недоцільним запропонований С. Макаренком поділ інформаційних операцій за метою та завданнями на інформаційне забезпечення, СІО та інформаційне протиборство [5], адже в сучасних умовах СІО з високою результативністю застосовуються саме як інструмент інформаційного протиборства).

Наразі Доктрина інформаційної безпеки України передбачає, що Міністерство оборони України та Генеральний штаб Збройних Сил України відповідно до компетенції забезпечують протидію СІО, спрямованим проти Збройних Сил України та інших військових формувань, супроводження інформаційними засобами виконання завдань оборони України, а Служба безпеки України протидіє проведенню проти України СІО, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій [10]. Втім згадана Доктрина жодним чином не регламентує власне проведення СІО та не дає уявлення про їхню сутність. Певною мірою цю прогалину усуває Воєнна доктрина України, яка опосередковано визначає СІО як елемент стратегічних комунікацій.

Зокрема, у ч. 16 ст. 4 розділу 1 Воєнної доктрини України зазначається, що стратегічні комунікації визначаються як скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави [11]. Втім таке визначення одночасно додає нових питань в частині розуміння СІО як правового феномену, зокрема – у чому полягає різниця між інформаційними і психологічними операціями, і чи не може за допомогою СІО відбуватися просування цілей держави.

Слід зауважити, що спираючись на стандарти НАТО науковці вирізняють серед компонентів системи стратегічних комунікацій безпосередньо інформаційні операції

(Information Operations) та психологічні операції (PSYOPS), однак до проведення СІО можуть мати безпосереднє відношення також інші компоненти цієї системи, зокрема:

- інформаційні заходи міжнародного військового співробітництва (International Military Cooperation);
- дії в кіберпросторі, включаючи соціальні мережі;
- залучення ключових лідерів до проведення інформаційних заходів (Key Leaders Engagement);
- інформування про ситуацію (Visual Info/Situation Awareness);
- документування подій на полі бою (Combat Camera);
- розвідувальне забезпечення проведення інформаційних заходів;
- демонстрація дій військ (Show of Force);
- введення в оману (MILDEC);
- безпека операцій (Operation Security);
- протиборство в електромагнітному просторі (EMW) тощо [12 – 15].

СІО можуть носити як інформаційно-технічний, так і інформаційно-психологічний характер, охоплюючи всі напрямки інформаційного протиборства.

При інформаційно-технічній боротьбі головними об'єктами впливу й захисти є інформаційно-технічні системи (системи зв'язку, телекомунікаційні системи, радіоелектронні засоби тощо). Інформаційно-технічний вплив є цілеспрямованим виробництвом і поширенням спеціальної інформації, яка безпосередньо впливає на функціонування й розвиток інформаційно-технічного середовища суспільства, тобто комп'ютери, засоби зв'язку й програмне забезпечення, що відіграють роль зброї масового знищення, за допомогою якої можна проникати в комп'ютерні системи й порушувати їхню роботу. Основна роль у цьому приділяється руйнівним атакам на критичну інфраструктуру супротивника.

При проведенні СІО інформаційно-психологічного характеру (саме їх зазвичай розуміють як класичні приклади СІО) основними об'єктами впливу стають психіка представників політичної еліти й населення конфронтуючих держав, а також система формування суспільної свідомості, думки й прийняття державно-управлінських рішень у сфері національної безпеки. СІО психологічної спрямованості, таким чином, становить цілеспрямоване виробництво й поширення спеціальної інформації, яка безпосередньо впливає (позитивно або негативно) на функціонування й розвиток інформаційно-психологічного середовища суспільства, психіку й поведінку політичної еліти й населення конкретної країни.

Як зазначають В. Фурашев та Д. Ланде, зміст СІО спрямований на реалізацію попередньо спланованих психологічних дій в мирний і воєнний час на ворожу, дружню або нейтральну аудиторію засобами впливу на настанови та поведінку з метою досягнення політичних або воєнних переваг. Ці операції поєднують психологічні дії зі стратегічними цілями, психологічні консолідуючі дії та психологічні дії з безпосередньої підтримки бойових дій.

Основне завдання інформаційних операцій полягає у маніпулюванні масами на рівні суспільної та індивідуальної свідомості найчастіше з метою:

- внесення у свідомість ворожих, шкідливих ідей та поглядів;
- дезорієнтації та дезінформації мас;
- послаблення певних переконань, устоїв;
- залякування свого народу образом ворога;
- залякування супротивника своєю могутністю;
- забезпечення ринку збуту для своєї економіки [16, с. 49-50].

Квінтесенцією інформаційного забезпечення СІО інформаційно-психологічного характеру є їх інформаційний етап, тож на його дослідженні зупинимось детальніше.

Інформаційний етап СІО передбачає створення чи/та вибір інформаційного приводу як тригеру (автоматичні поведінкові реакції людини, що виникають у відповідь на яку-небудь подію) [17 – 19] для всієї операції. Саме від правильного вибору інформаційного тригеру залежить інформаційний розвиток ситуації навколо явища, процесу чи події, які є базою СІО. За своєю суттю інформаційний привід покликаний мотивувати чи демотивувати суб'єктів СІО (особу чи коло осіб) до вчинення певних дій чи до бездіяльності відповідно до намірів, цілей та оперативного задуму організаторів операції.

Загалом, у плануванні ІПВ можна користуватись схемою, яку використовують засоби масової інформації (далі – ЗМІ) з метою "зачепити" користувача та утримати його увагу. Найбільш активно сучасні ЗМІ використовують схему "СССССГ", де відповідно: "Скандали, Сенсації, Страх, Секс, Смерть, Сміх та Гроші" [20]. Кожна із зазначених тем викликають окрему, специфічну реакцію в аудиторії, що і є головною метою інформаційного етапу СІО у процесі підбору чи створення інформаційного приводу. Саме запланованe емоційне забарвлення інформаційного приводу визначає наміри щодо подальшого розвитку самої СІО та ситуації навколо об'єкту СІО. Тож завдання організаторів СІО – у підготовчому етапі визначити домінантний тип емоційного стану цільової аудиторії, а у випадку відсутності можливості (під час інформаційного етапу, перед проведенням інформаційного приводу) – здійснити комплекс інформаційних акцій, які створять необхідний емоційний стан або підсилять наявний емоційний стан, необхідний для подальшого ефективного інформаційного етапу.

Інформаційний привід є невід'ємною частиною СІО і повинен бути тісно пов'язаний з третім етапом операції – закріпленням результатів ІПВ, оскільки інформаційний привід є тригером до дії чи бездіяльності цільової аудиторії в рамках СІО, адже саме дія чи бездіяльність і є головною метою ІПВ, результати якого фіксуються у закріплювальному етапі СІО.

У якості прикладу інформаційного приводу в СІО пропонуємо розглянути СІО "Гюльчатай" (далі – операція), яка була проведена міжнародним центром "Миротворець" [21 – 22].

Навесні 2015 року невідомими (на той момент) було вбито проросійського журналіста та публіциста Олеся Бузину (16.04.2015 р.) та колишнього народного депутата від Партії регіонів, Олега Калашнікова (15.04.2015 р.). Адміністраторами однойменного сайту центру "Миротворець" "заднім числом" було розміщено на сайті профілі персональних даних, вбитих з місцями проживання, фотографіями, контактними даними тощо, а опісля – розміщено статтю про нагороду "агента 404" (404 – це код помилки, що міститься у відповіді сервера на запит користувача та свідчить про відсутність запитуваної інформації на сервері – *прим. Авт.*) за успішну ліквідацію зазначених осіб. Інформація про це (стосовно розміщення профілю, подальшого вбивства та "нагородження агента") була широко поширена серед проросійськи налаштованих користувачів мережі Інтернет та дійшла до потенційних і чинних на той момент членів терористичних організацій "Луганська народна республіка", "Донецька народна республіка" та інших афілійованих до них бандитських угруповань та злочинців.

Оскільки доступ пересічному користувачу мережі Інтернет до бази даних терористів та осіб, що підозрюються у співпраці з терористичними організаціями та з країною-агресором (Російська Федерація), що розміщена на сервері центру

“Миротворець”, можливий лише через форму пошуку, особи, що потенційно можуть бути у зазначеній базі та переймались за свою безпеку (А. Медведько та Д. Поліщук, підозрювані у вбивстві О. Бузини, були затримані значно пізніше) могли пересвідчитись про наявність чи відсутність своїх даних у зазначеній базі лише після того, як власноруч введуть свої ім’я та прізвище. У свою чергу, адміністратори сайту “Миротворець” мають можливість фіксувати всі дані, що вводяться користувачами у форму пошуку (ім’я, по-батькові, прізвище, позивний тощо) та, користуючись технологією OSINT (одна з розвідувальних дисциплін. Включає в себе пошук, вибір і збір інформації, отриманої із загальнодоступних джерел і її аналіз), проводити подальше наповнення бази новими підозрюваними у тероризмі та співпраці з терористичними організаціями.

Таким чином, операція публічно складалась з наступних етапів

1. Підготовчий етап. Фактично, підготовчий етап у цієї конкретній операції відсутній, оскільки організатори використали наявний інформаційний привід та наявні адміністративні та оперативні ресурси, напрацьовані попередніми операціями.

2. Інформаційний привід. Використано наявну подію, гучне вбивство. Повертаючись до вищенаведеної схеми, тема підпадає під ознаки *“сенсація”* (смерть проросійськи налаштованих широковідомих осіб). Варто зазначити, що така ситуація (майже одночасна смерть відомих опозиційних, радикально проросійських медійних особистостей) виникла вперше у новітній історії України. Представники центру “Миротворець” додали елемент *“страх”*, увівши неіснуючого агента “404” із натяком на те, що будь-яка особа, яка перебуває в базі центру “Миротворець”, є під загрозою фізичної ліквідації. Завдяки комплексу дій з боку центру “Миротворець” відомостями, стосовно наявності профілю персональних даних, зазначених осіб було широко поширено серед проросійської аудиторії, в тому числі такі відомості були поширені центральними ЗМІ РФ та популярними проросійськими й російськими блогерами і журналістами. Тим самим, посіявши панічні настрої серед потенційних учасників бази центру “Миротворець” та спровокувавши їх на наступну дію, пошук самих себе на сайті центру “Миротворець” стало наступним етапом операції “Гюльчатай”.

3. Закріплювальний етап. Особи, які відносили себе до тих, хто може бути у базі центру “Миротворець” та переймались за власну безпеку й маючи доступ до бази виключно через форму пошуку на сайті, почали активно шукати себе у зазначеній базі, тим самим власноруч вносили свої персональні дані (прізвище, ім’я, по-батькові, позивний) у цю базу, мимовільно надаючи команді центру “Миротворець” відомості про себе. Це розширення бази і було ціллю операції. Побічним та корисним результатом операції було поширення страху, демонізація центру “Миротворець” в очах терористів та їхніх поплічників, що розширило можливості та цінність центру “Миротворець”.

4. Вихід з операції. Після того, як командою центру “Миротворець” було зібрано достатньо інформації, на сайті проекту було розміщено відомості про операцію, її цілі завдання та перебіг із саркастичною подякою всім її учасникам з числа терористів та їх прибічників.

З використанням НЛП-теорії про референтний стан мас можна зробити такий висновок, що в даному випадку цільова аудиторія гучною подією була введена в стан пасивного негативу (жах від інформації про смерть О. Бузини та О. Калашнікова) а представниками центру “Миротворець” доведена до стану активного негативу – страх за власне життя, що штовхнуло потенційних (на їхню власну думку) жертв “агента 404” на пошук самих себе у базі центру “Миротворець”.

Отже, фактично перед організаторами СІО стоїть завдання започаткування контрольованого поширення та направлення психічної енергії в руслі, відповідно до

задуму організаторів операції. Варто зазначити, що у суспільстві одночасно обертається велика кількість інформації, адже відбувається політична боротьба, протидія гібридній агресії РФ, країна переживає економічну кризу тощо, відповідно населення постійно перебуває під постійним зовнішнім психологічним тиском. Більше того, цей тиск на суспільство відбувається масовано і комплексно, з різних джерел (ЗМІ, соціальні мережі, чутки тощо) та цілодобово отже як для інформаційних операцій, так і для інформаційних приводів виникають чи можуть виникнути будь-які обставини, які у свою чергу можуть вилитися у будь-які ситуації, і не тільки спецслужби, але й треті сторони можуть їх використати у своїх цілях.

В цілому формалізація етапів проведення СІО на теоретичному рівні має синхронізуватися із вдосконаленням нормативно-правового підґрунтя їх проведення, котре, як вже зазначалося вище, наразі не може вважатися не лише досконалим, але й елементарно достатнім. Доцільним у подальшому вдосконаленні нормативно-правового регулювання СІО вважаємо орієнтування на стандарти НАТО, перевагою яких є впровадження у практику планування та проведення СІО детального аналізу комплексу факторів обстановки, механізмів координації складових сектору безпеки і оборони та інших державних органів, групових методів роботи, відпрацьованих й перевірених провідними зарубіжними країнами при забезпеченні національної безпеки прийомів й способів інформаційного впливу [9, с. 153-154].

Висновки.

Наразі важливо передусім визначити сутність та місце СІО в системі засобів забезпечення інформаційної та національної безпеки України в цілому, а також окреслити основні вимоги до їх проведення (з урахуванням специфіки всіх основних етапів СІО) з метою забезпечення балансу інтересів національної безпеки та дотримання прав і свобод людини й громадянина, унеможливлення використання інформаційних потужностей для провокації злочинів тощо.

Необхідно враховувати, що у розробці та проведенні СІО інформаційний привід посідає одне з найважливіших місць у операції, оскільки він є точкою входу в процес мотивації чи демотивації цільової аудиторії відповідно до оперативного задуму, цілей та завдань організаторів СІО, які відображаються у наступному етапі операції – фіксувальному, який є віддзеркаленням всієї операції у якому цільова аудиторія здійснює чи відмовляється від здійснення своїх дій, відповідно до оперативного задуму, цілей та завдань організаторів СІО.

Відповідно, правильний та коректний підбір наявного інформаційного приводу чи створення нового інформаційного приводу є одним із найважливіших етапів у проведенні СІО. При цьому впровадження сектором безпеки і оборони України методології проведення СІО, яка використовується у країнах НАТО, та нормативно-правове закріплення відповідних стандартів значно посилить спроможності нашої держави у веденні інформаційного протиборства в умовах гібридної війни.

Використана література

1. Arquilla J., Ronfeldt D. The Emergence of Noopolitik: Towards an American Information Strategy. RAND/MA-103305D. 1999. 102 p.

2. Гриняев С.Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. Москва, 2004. 428 с.

3. Черных С.Н., Зуева Н.А. Информационная война: традиционные методы, новые тенденции. *Контекст и рефлексия: философия о мире и человеке*. 2017. Т. 6. № 6А. С. 191-199.

4. Литвиненко О.В. Інформаційні впливи та операції. Київ: ВКФ. Сатсанга, 2003. 240 с.

5. Макаренко С. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. URL: https://psyfactor.org/t/Makarenko_InfPro_2017.pdf (дата звернення: 03.12.2018).

6. Козирацкий Ю.Л., Прохоров Д.В., Козирацкий А.Ю., Голубев С.В. Основы информационной и радиоэлектронной борьбы: учебное пособие. Воронеж: ВАИУ, 2009. 192 с.

7. Иванов И., Чадов И. Содержание и роль радиоэлектронной борьбы в операциях XXI века. *Зарубежное военное обозрение*. 2011. № 1. С. 14-20. URL: http://militaryarticleru/zarubezhnoe-voennoe-obozrenie/2011-zvo/8094-soderzhanie-i-rol-radiojelektronnoj-borby-v (дата звернення 02.12.2018).

8. Панченко В.М. Інформаційні операції в асиметричній війні Росії проти України: підходи до моделювання. *Інформація і право*". № 3(12)/2014. С.13-16.

9. Заруба О.Г. Планування спеціальних інформаційних операцій. *Інформаційна безпека людини, суспільства, держави*. 2017. № 1(21). С.140-154.

10. Доктрина інформаційної безпеки України: затверджена Указом Президента України "Про рішення Ради національної безпеки і оборони України від 29.12.16 р. "Про Доктрину інформаційної безпеки України". URL: http://www.president.gov.ua/documents/472017-21374 (дата звернення 28.11.2018).

11. Про рішення Ради національної безпеки і оборони України "Про нову редакцію Воєнної доктрини України": Указ Президента України від 2.09.15 р. № 555/2015: http://www.president.gov.ua/documents/5552015-19443 (дата звернення: 30.11.2018).

12. Кушнір О.В. Поняття та сутність стратегічних комунікацій у сучасному українському державотворенні. URL: http://goal-int.org/ponyattya-ta-sutnist-strategichnix-komunikacii-u-suchasnomu- ukrainskomu-derzhavotvorenni (дата звернення: 04.12.2018).

13. Ліпкан В.А. Сутність гібридної війни проти України. *Імперативи розвитку цивілізації*. 2015. № 2. С. 13-16.

14. Ліпкан В.А. Роль стратегічних комунікацій в протидії гібридній війні проти України. URL: http://goal-int.org/rol-strategichnix-komunikacij-v-protidii-gibridnij-vijni-proti-ukraini (дата звернення 30.11.2018).

15. Daniel Gage. The continuing evolution of Strategic Communication within NATO. *The Three Swords Magazine*. 27/ 2014. P. 53-55.

16. Фурашев В.М., Ланде Д.В. Інформаційні операції крізь призму системи моніторингу та інтеграції інтернет ресурсів. *Правова інформатика*". № 2(22)/2009. С. 49-57.

17. Богданова Ю.О. Психология маркетинга. URL: http://www.aup.ru/books/m500; http://www.gumer.info/bibliotek_buks/psihol/olshansk/15.php (дата звернення: 30.11.2018).

18. Резепов И. Психология рекламы и PR. URL: http://www.e-reading.club/book.php?book=89173 (дата звернення: 29.11.2018).

19. Лизанчук В. Психологія мас-медіа. URL: http://journ.lnu.edu.ua/books/ps-mas-media.pdf (дата звернення: 05.12.2018).

20. Сім орієнтирів "ТСН": Скандали, Сенсації, Страх, Смерть, Секс, Сміх і Гроші. URL: http://ru.telekritika.ua/redpolitics/2008-06-04/38798 (дата звернення: 03.12.2018).

21. Спецоперация "Гюльчатай, открой личку!" или сказ о том, как мы "разводили" вату, пользуясь методами российских пропагандистских СМИ. Ч. 1. URL: https://psb4ukr.org/189342-specoperaciya-gyulchataj-ili-skaz-o-tom-kak-my-razvodili-vatu (дата звернення: 04.12.2018).

22. Спецоперация "Гюльчатай, открой личку!" или сказ о том, как мы "разводили" вату, пользуясь методами российских пропагандистских СМИ. Ч. 2. URL: https://psb4ukr.org/190529-specoperaciya-gyulchataj2 (дата звернення: 04.12.2018).

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

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

УДК 351.751

НИЖНИК А.І., *заслужений юрист України*

СУЧАСНІ ТЕНДЕНЦІЇ НАДАННЯ КОМІТЕТАМ ВЕРХОВНОЇ РАДИ УКРАЇНИ СПЕЦІАЛЬНИХ ПОВНОВАЖЕНЬ ДЛЯ ЗДІЙСНЕННЯ ПАРЛАМЕНТСЬКОГО КОНТРОЛЮ: ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *Статтю присвячено дослідженню тенденцій законодавчого удосконалення організації парламентського контролю в Україні. У межах викладеного матеріалу проаналізовано недоліки конституційного та законодавчого регулювання організації парламентського контролю, запропоновано варіант їх усунення на конституційному рівні з урахуванням парламентської практики.*

Ключові слова: *парламентський контроль, комітети Верховної Ради України.*

Summary. *This article is devoted to the study of current trends in legislative improvement of the organization of parliamentary control in Ukraine. Within the framework of the material presented, the shortcomings of the constitutional and legislative regulation of the organization of parliamentary control are analyzed, the option of eliminating them at the constitutional level is proposed (taking into consideration recent parliamentary practice).*

Keywords: *parliamentary control, Committees of the Verkhovna Rada of Ukraine.*

Аннотация. *Статья посвящена исследованию тенденций законодательного совершенствования организации парламентского контроля в Украине. В рамках изложенного материала проанализированы недостатки конституционного и законодательного регулирования организации парламентского контроля, предложен вариант их устранения на конституционном уровне с учетом парламентской практики.*

Ключевые слова: *парламентский контроль, комитеты Верховной Рады Украины.*

Постановка проблеми. За нинішнього низького рівня довіри до влади та існуючого стану громадського контролю роль парламентського контролю в Україні набуває неабиякого значення. Адже загальновідомо, що, обираючи парламентаріїв, виборці делегують їм від імені Українського народу право на здійснення парламентського контролю.

Існуюча нині конституційна модель парламентського контролю зумовлює його здійснення Верховною Радою України за допомогою утворюваних нею органів – комітетів і тимчасових комісій. Ключову роль у процесі парламентського контролю відіграють парламентські комітети.

Результати аналізу наукових публікацій. Проблематиці реалізації функції парламентського контролю присвячено багато досліджень. Зокрема, О.В. Висовень, І.К. Залюбовська, С.В. Ківалов, О.О. Майданник, М.П. Орзіх вважають, що комітети Верховної Ради України виконують повноваження парламентського контролю неналежним чином з причин недостатньої уваги, яка приділяється реалізації ними саме цих повноважень; внаслідок рекомендаційного, а не обов'язкового характеру рішень комітетів; через відсутність спеціального законодавчого регулювання у цій сфері

суспільних відносин (зокрема на рівні окремого закону про парламентський контроль в Україні або про засади парламентського контролю в Україні, законопроектні розробки з якого безуспішно проводилися у Верховній Раді України протягом 1999 – 2006 років) [1 – 5].

Інші дослідники звертають увагу на: відсутність чітких конституційних норм, які б дозволяли реалізовувати парламентський контроль у межах діяльності комітетів Верховної Ради України (І.К. Залюбовська, О.О. Майданник, М.П. Орзіх, Є.А. Тихонова) [6 – 9]; неефективність і вибірковість, відсутність постійності і системності у контрольній діяльності комітетів Верховної Ради України; недостатню реалізацію ними існуючих можливостей при здійсненні парламентського контролю [10]).

За висновком Ю.С. Шемшученка, неоднозначність положень самої Конституції України не дозволяє повною мірою реалізувати контрольну функцію парламенту України, що є причиною невиконання законів, безвідповідальності в діяльності органів виконавчої влади в цілому [11].

Питання реалізації функції парламентського контролю розглянуто у науковій статті М.О. Теплюка, у якій зазначено, що парламентський контроль може мати різний обсяг, залежно від форми правління в державі, а також державотворчих традицій. Наголошено, що найбільш сильний парламентський контроль притаманний державам з парламентською формою правління та окреслено основні проблеми на шляху до посилення системи парламентського контролю в Україні, зокрема: "…парламентський контроль в існуючих умовах поділу влади, будучи одним із механізмів "стримувань і противаг" між гілками влади, не передбачає прямого втручання парламенту в безпосередню діяльність глави держави, державних органів. У демократичних державах парламентський контроль є механізмом реальної політики, у той час як в умовах авторитарних і тоталітарних режимів контрольні повноваження парламентів, по суті, виявляються фіктивними" [12, с. 463-464].

Майданник О.О. наголошує на тому, що "конституційна й законодавча регламентація контрольних повноважень парламенту України вимагає подальшого розвитку й вдосконалення"; "вирішення існуючих проблем законодавчого забезпечення реалізації парламентом України функції контролю стане важливим засобом зміцнення демократичної конституційної законності в діяльності всіх владних і самоврядних структур і, в свою чергу, буде сприяти підвищенню ефективності у здійсненні Українським парламентом законодавчої й інших його функцій та створенню більш дійової і ефективної законодавчої бази країни" [13].

Як бачимо, питання можливості функціонування в Україні парламентських комітетів як суб'єктів владних повноважень вітчизняними науковцями не досліджувалося. Принаймні за допомогою Інтернет-ресурсів досліджень на таку тему не виявлено.

Метою статті є виявлення сучасних тенденцій законодавчого удосконалення ефективності парламентського контролю з боку комітетів Верховної Ради України шляхом наділення того чи іншого парламентського комітету спеціальним контрольним повноваженням. Питання фактичних передумов, у тому числі політичної доцільності вжиття законодавцем подібних кроків, винесені за межі цієї статті.

Виклад основного матеріалу. Насамперед маємо констатувати, що на нинішньому етапі реформування український народ (єдине джерело влади) та держава здійснюють державотворчі кроки в умовах недовершеної конституційної реформи.

Якщо керуватися текстом Конституції України [14]в редакції Закону від 21.02.2014 р. № 742-VII[1], то наразі в Україні існує парламентсько-президентська форма правління.

Конституційно-правовий статус, зокрема комітетів і спеціальних комісій українського парламенту, визначено статтею 89 згаданого тексту Конституції України. Згідно з її редакцією Верховна Рада України для здійснення законопроектної роботи, підготовки і попереднього розгляду питань, віднесених до її повноважень, ***виконання контрольних функцій відповідно до Конституції України*** створює з числа народних депутатів України комітети Верховної Ради України.

Відповідно до останньої частини статті 89, організація і порядок діяльності комітетів Верховної Ради України, її тимчасових спеціальних і тимчасових слідчих комісій встановлюються законом. Отже, як бачимо, у змісті цієї статті немає навіть натяку на самостійні повноваження парламентських комітетів. І це цілком природно. Адже з огляду на їхній конституційно-правовий статус вони, на відміну від Верховної Ради України, не є органами державної влади. Принаймні серед вітчизняних досліджень, що присвячені питанням правової природи комітетів парламенту та були зроблені до появи нового Закону України "Про національну безпеку", мною не виявлено протилежної точки зору, а в судовій практиці не було випадків, коли парламентський комітет визнали б суб'єктом владних повноважень [19].

Аби збагнути відмінність конституційного регулювання парламентського контролю, варто проаналізувати у системному взаємозв'язку нинішню редакцію положень статей 85 і 89 Конституції та порівняти їхній зміст з попередньою редакцією.

Існуюча на сьогодні редакція пунктів 13 і 33 частини першої статті 85, статті 89 Конституції України збігається з редакцією цих самих положень, що вперше з'явилися у тексті Основного Закону України згідно із законом від 8 грудня 2004 року № 2222. Саме цим Законом було відкориговано пункт 13 частини першої статті 85 Конституції України щодо здійснення Верховною Радою України контролю за діяльністю Кабінету Міністрів України відповідно до цієї Конституції (законодавцем після слів "цієї Конституції" було доповнено словами "та закону") та пункт 33 частини першої статті 85 Конституції України щодо здійснення парламентського контролю у межах, визначених цією Конституцією (законодавцем після слів "цією Конституцією" було доповнено словами "та законом"). Оскільки частина перша статті 85 присвячена визначенню переліку повноважень Верховної Ради України, то поява у зазначених пунктах слів "та закону" є лише невдалою законодавчою спробою розширити через закон (можливо про Верховну Раду, оскільки згідно з пунктом 15 частини першої статті 85 Регламент Верховної Ради не є законом?) межі парламентського контролю з боку парламенту. У будь-якому разі оновлена редакція пунктів 13 і 33 частини першої статті 85 Конституції України не може тлумачитися так, що в них йдеться про парламентські комітети як самостійні суб'єкти парламентського контролю.

Хоча положення статті 89 Конституції України, на відміну від положень її статті 85, і присвячено питанням організації та порядку діяльності комітетів, тимчасових спеціальних і тимчасових слідчих комісій, проте у змісті частини першої статті 89 згадки про закон немає. Відтак, небезспірною виглядає юридична позиція щодо можливості наділення у законі парламентського комітету спеціальними контрольними повноваженнями. Адже ні про які контрольні **повноваження комітетів** парламенту у статті 89 не йдеться. І це цілком природно, зважаючи на існуючий конституційний статус парламентських комітетів.

[1] *Відомості Верховної Ради України*. 2014. № 11. Ст. 143.

На жаль, на сьогодні не існує рішень Конституційного Суду України про тлумачення положень статей 85 і 89 Конституції України протягом їхньої дії як у редакції Закону від 08.12.2004 р. № 2222-IV, так і в редакції Закону від 21.02.2014 р. № 742-VII.

Разом з тим, у результаті функціонування в Україні органу конституційної юрисдикції маємо його правові позиції, які стосуються невірної інтерпретації відповідних конституційних положень у контексті законодавчого регулювання організації парламентського контролю.

Насамперед це стосується оцінки Конституційним Судом України деяких положень нової редакції Закону України "Про комітети Верховної Ради України", ухваленої 22 грудня 2005 року у розвиток оновлених положень Конституції України в редакції Закону від 08.12.2004 р. № 2222-IV [15].

Так, наприклад, Конституційний Суд України, детально дослідивши теоретичні обґрунтування природи парламентського контролю, висловився щодо змісту та обсягу контрольних повноважень комітетів Верховної Ради України у своєму Рішенні від 10 червня 2010 р. № 16-рп/2010. У ньому, зокрема, зазначено, що Основний Закон України не наділяє комітети самостійними контрольними повноваженнями, вони можуть лише сприяти Верховній Раді України у здійсненні повноважень щодо парламентського контролю, виконуючи певні дії допоміжного (інформаційного, експертного, аналітичного тощо) характеру. Оскільки повноваження Верховної Ради України визначаються виключно Основним Законом України, наявність цих конституційних приписів дає підстави для висновку про неможливість наділення парламенту та його органів повноваженнями надавати згоду іншим органам державної влади на кадрові рішення, не передбачені в Конституції України [16].

У Рішенні ж № 12-рп/2009 Конституційний Суд України на підставі аналізу конституційних та законодавчих положень, які врегульовують питання діяльності комітетів Верховної Ради України, зробив, зокрема, висновок про відсутність у комітетів Верховної Ради України повноваження погоджувати призначення на посади і звільнення з них тих чи інших посадових осіб, а також надавати згоду на створення і ліквідацію спеціальних підрозділів відповідних правоохоронних органів. Діяльність комітетів пов'язана з вирішенням лише на стадії підготовки та попереднього розгляду питань, віднесених до повноважень Верховної Ради України. Вони не можуть виконувати свої організаційні функції з кадрових питань в інший спосіб, ніж шляхом здійснення підготовчої роботи для призначення, звільнення, затвердження та надання згоди на призначення посадових осіб Верховною Радою України. Оцінюючи ці положення, Конституційний Суд України вбачає, що функції, які стосуються кадрових питань, віднесені законодавцем не до контрольних, а до організаційних [17].

Формулювання згаданих позицій єдиним органом конституційної юрисдикції в Україні не лише засвідчило неоднозначність у розумінні законодавцем та суб'єктами правозастосовної діяльності особливостей контрольної функції комітетів Верховної Ради України, а й дало змогу суттєво уточнити зміст відповідних конституційних положень.

Можна констатувати, що правові позиції Конституційного Суду України, які стосуються парламентського контролю та були ним висловлені у період дії відповідних положень Конституції України зразка 1996 і 2004 років (в редакції Закону від 21.02.2014 р. № 742-VII) сформували конституційну доктрину такого контролю.

У результаті їхнього узагальнення можна зробити такі висновки:

1) комітети Верховної Ради України є її допоміжними органами і водночас однією з організаційних форм парламентської діяльності, яка здійснюється на основі визначеної статусним законом універсальної компетенції, що органічно пов'язана з конституційними повноваженнями Верховної Ради України;

2) робота комітетів в аспекті контрольної функції Верховної Ради України не має самостійного характеру і здійснюється у межах предметів їх відання;

3) існуючий конституційний статус комітетів Верховної Ради України, що окреслює цільове призначення їхньої діяльності, унеможливлює існування спеціального контрольного комітету.

Натомість поточне законодавче регулювання організації і порядку діяльності парламентських комітетів (Закон України "Про комітети Верховної Ради України", Закон про Регламент Верховної Ради України, інші закони) виходить з концепції існування відносно самостійної контрольної функції комітетів Верховної Ради України, що зазвичай помилково ототожнюється з їх контрольними повноваженнями.

Так, на сьогодні організацію і порядок діяльності комітетів Верховної Ради України унормовано Законом України "Про комітети Верховної Ради України"[2]. Його положення мають універсальний характер для всіх парламентських комітетів, зважаючи на їх однаковий конституційно-правовий статус.

Згідно зі статтею 11 цього Закону комітети Верховної Ради України здійснюють такі функції: законопроектну, організаційну, контрольну. Однак, як вже зазначалося Конституцією України (статті 19 і 85), реалізація контрольної функції покладена інституційно на Верховну Раду України, а її комітети в межах предметів їх відання лише здійснюють законопроектну роботу, підготовку і попередній розгляд питань, віднесених до повноважень парламенту (стаття 89).

Способи ж реалізації комітетами контрольної функції, котрі не можна ототожнювати з повноваженнями, що притаманні органам державної влади, визначено статтею 14 зазначеного Закону, а відповідний набір прав і обов'язків комітетів Верховної Ради України при здійсненні контрольної функції міститься у главі 3 розділу ІІІ цього Закону**.** Тут доречно нагадати про долю пункту 10, яким статтю 14 було доповнено Законом від 23.10.2009 р. № 1692-VI і положення якого втратили чинність як такі, що є неконституційними, на підставі Рішення Конституційного Суду України №16-рп/2010 [18].

Протягом дії цього положення контрольна функція комітетів полягала, зокрема, у погодженні питань, проведенні консультацій щодо призначення на посади та звільнення з посад керівників відповідних державних органів, створенні і ліквідації спеціальних державних органів, що віднесені до предметів відання комітетів, та здійсненні інших погоджень і консультацій у випадках, передбачених законом.

Разом з тим, у тексті закону про комітети (статті 2, 4, 13) помилково вжито термін "повноваження", тоді як у контексті здійснення комітетами законопроектної, організаційної чи контрольної функцій йдеться про межі "предмета їх відання".

Як відомо, у всіх скликаннях Верховної Ради України функціонувала Спеціальна контрольна комісія з питань приватизації, існування якої всупереч проаналізованим конституційним положенням було передбачено статтею 10 Закону України "Про приватизацію державного майна"[3], а зараз статтею 9 Закону України "Про приватизацію

[2] *Відомості Верховної Ради України.* 1995. № 19. Ст. 134.

[3] *Відомості Верховної Ради України.* 1992. № 24. Ст. 348.

державного і комунального майна”[4]. Адже, якщо керуватися логікою частини другої статті 89 Конституції України та положеннями Закону України “Про Регламент Верховної Ради України”, то функціонування тимчасової спеціальної комісії обмежене в часі одним роком (частина восьма статті 85 Регламенту), що унеможливлює її функціонування протягом всього періоду діяльності парламенту відповідного скликання.

Отже, законодавець, ухваливши 18 січня 2018 року Закон України “Про приватизацію державного і комунального майна”, інакше витлумачив положення статті 89 Конституції України, перебравши на себе виключне повноваження Конституційного Суду України щодо офіційного тлумачення Основного Закону України (пункт 2, частини першої статті 150 Конституції України).

Незважаючи на можливість настання наслідків, про які йдеться у статті 152 Конституції України (в редакції Закону від 2 червня 2016 р. №1401-VIII), Верховна Рада 21 червня 2018 року ухвалила новий Закон “Про національну безпеку України”, положення статті 6 якого присвячено питанням парламентського контролю.

Зокрема, абзацом другим частини другої цієї статті передбачено:

“З метою гарантування неухильного і безумовного дотримання державними органами спеціального призначення з правоохоронними функціями, правоохоронними органами, правоохоронними органами спеціального призначення та розвідувальними органами вимог Конституції України щодо забезпечення національної безпеки створюється комітет Верховної Ради України, до повноважень якого належить забезпечення контрольних функцій Верховної Ради України за діяльністю цих органів. **Завдання та повноваження** цього комітету Верховної Ради України визначаються законом”.

Ця редакція повністю збігається з тією, що була у внесеному Президентом України законопроекті (від 28.02.2018 р. № 8068) та схвалена парламентом у першому читанні. Після прийняття його як закону та підписання Президентом України як гарантом додержання Конституції України, глава держави взяв цей Закон до виконання (частина друга статті 94 Конституції України).

Чи означає це, наприклад, що у щільному робочому графіку Президента України знайдеться час, щоб невідкладно з’явитися на засідання такого спеціального комітету? З огляду на парламентську практику схиляюся до думки, що цей обов’язок виконуватиме представник Президента України, та чи буде він настільки обізнаний у таких специфічних питаннях? Які заходи впливу (санкції) згідно із законом комітет зможе застосувати стосовно підконтрольних суб’єктів? Адже у випадках виявлення порушень законодавства у діяльності підконтрольного суб’єкта, парламентом мають бути вжиті відповідні заходи.

Отже, йдеться про створення у системі існуючих “класичних” комітетів спеціального контрольного комітету, що законом буде наділений специфічними завданнями та повноваженнями, які гарантуватимуть належний цивільний демократичний контроль над сектором безпеки і оборони України з боку Верховної Ради України. Наразі ця контрольна функція здійснюється комітетом з питань національної безпеки і оборони. Відтак, новий комітет має отримати через закон спеціальні форми та засоби здійснення ним парламентського контролю, що по суті може перетворити його на міні-парламент.

---

[4] *Відомості Верховної Ради України.* 2018. № 12. Ст. 68.

За такого законодавчого підходу спотворюється зміст статті 89 Конституції України та порушується принцип рівності комітетів, а спроба штучного посилення ефективності парламентського контролю на рівні комітету робить такий комітет більш впливовим і привабливим для народних депутатів. Однак до визначення законом так званих повноважень цього комітету виникає питання – чи здійснюватиме він також і законопроектну роботу? Можливо, це спроба запозичення досвіду Національних зборів Коста-Ріки, де система комітетів складається із комітетів, що мають право фактично ухвалювати закони або вносити до них зміни з певних питань незалежно від їхнього розгляду законодавчим органом у цілому; "класичних" комітетів, що виконують звичну роль, обговорюючи, формулюючи і пропонуючи законопроекти на розгляд всього парламенту; і окремих комітетів, які не мають права вносити законопроекти, а лише виконують контрольні функції і вважаються одними з найвпливовіших комітетів. Однак для запровадження подібної системи комітетів в українському парламенті (за умови наявності суспільної необхідності та нової доктрини парламентського контролю) необхідно було б у ході конституційної реформи змінити не лише дещо консервативний зміст статті 89 Конституції України, а й інших її положень, що стосуються парламентського контролю.

Звичайно, перед розробниками доктрини сучасного парламентського контролю "європейського зразка" виникне низка юридичних питань, зокрема:

– чи мають окремі парламентські комітети бути квазі-суб'єктами владних повноважень, а їхні акти, дії чи бездіяльність підпадати під судовий контроль;

– якими спеціальними (додатковими) контрольними повноваженнями має наділятися комітет порівняно з тими, що нині визначені у Законі "Про комітети Верховної Ради України".

А оскільки технічне завдання полягатиме у розбудові в Україні моделі парламентського контролю саме "європейського зразка", то учасникам вироблення нової доктрини варто орієнтуватися на досвід країн системи континентального права.

Зважаючи на останні тенденції посилення в Україні парламентського контролю у процесі євроінтеграційних перетворень, варто очікувати на нові наукові підходи щодо необхідності інституалізації парламентських комітетів як самостійних суб'єктів парламентського контролю на основі вітчизняних загальнотеоретичних засад розвитку парламентського контролю.

Висновки.

У ході цієї роботи проаналізовано зміст відповідних конституційних і законодавчих положень, правові позиції Конституційного Суду України та судів загальної юрисдикції. Зважаючи на обмежений обсяг статті, викладений у ній матеріал не претендує на повноцінне дослідження окресленої проблеми. Проте, вважаємо за необхідне зазначити наступне.

1. Викладений матеріал дозволяє дійти висновку, що законодавець, ігноруючи правові позиції органу конституційної юрисдикції, періодично (під час дії положень статей 85 і 89 Конституції України в редакції Закону від 08.12.2004 р. № 2222-IV та в редакції Закону від 21.02.2014 р. № 742-VII) здійснює спроби посилення парламентського контролю на рівні комітетів. При цьому глава держави, реалізуючи свої повноваження, передбачені статтею 94 Конституції України, діє як гарант її додержання, що обумовлює також врахування ним правових позицій Конституційного Суду України.

Подібні законодавчі експерименти, що виглядають як прогресивні, закономірно стають предметом уваги правників, експертів і врешті-решт Конституційного Суду України.

2. Для запровадження в Україні іншої системи парламентських комітетів, що передбачає функціонування спеціальних контрольних комітетів як самостійних суб'єктів парламентського контролю, має бути змінена редакція статті 89 та інших положень Конституції України в межах загальної концепції парламентської реформи та на основі сучасної доктрини державного управління.

3. На думку автора, для створення конституційних засад можливості функціонування більш оптимальної системи комітетів і комісій парламенту на нинішньому перехідному етапі, можна було б обмежитися коригуванням змісту частини другої та п'ятої статті 89 Конституції України. Зокрема, у частині другій мало б йтися про можливість створення спеціальних контрольних комісій, а зміст частини п'ятої міг би бути таким: "Організація, повноваження і порядок діяльності комітетів Верховної Ради України, її спеціальних контрольних комісій і тимчасових слідчих комісій, встановлюються законом та Регламентом Верховної Ради України".

Проте, оскільки за правилами юридичної техніки зміни до положень статті Основного закону України вносяться шляхом викладення її у новій редакції, новий зміст цієї статті, як такий, що перебуває у системному взаємозв'язку з іншими конституційними положеннями, може з'явитися лише в результаті здійснення конституційної реформи.

Використана література

1. Висовень О.В. Контрольні функції парламенту України як одна з умов його ефективної діяльності: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 393-395.

2. Залюбовська І.К. Парламентський контроль за діяльністю органів виконавчої влади як засіб забезпечення законності у сфері державного управління: автореф. дис. …канд. юрид. наук. – Одеса, 2002. С. 17.

3. Ківалов С.В. Парламентський контроль в Україні: законопроектні обґрунтування: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 411-417.

4. Майданник О.О. Теоретичні проблеми контрольної функції парламенту України: автореф. дис. …д-ра юрид. наук. Київ, 2008. С. 17.

5. Орзіх М.П. Функціональна характеристика парламентського контролю в Україні: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 441.

6. Залюбовська І.К. Законодавче забезпечення парламентського контролю за діяльністю органів виконавчої влади в Україні: сучасність та перспективи (проект Закону України "Про основні засади парламентського контролю в Україні"): зб. наук. праць *Актуальні проблеми держави і права*. Одеса, 2003. Вип. 19. С. 53-56.

7. Єрмолін В.П. Контроль за органами виконавчої влди як складова розвитку парламентаризму в Україні: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 404.

8. Майданник О.О. Деякі проблеми здійснення парламентського контролю: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 430.

9. Орзіх М.П. Функціональна характеристика парламентського контролю в Україні: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 437, 440-441.

10. Плахотнюк Н.Г. Контроль як провідна функція українського парламенту (організаційний аспект): матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 444-445.

11. Шемшученко Ю. Теоретичні засади розвитку українського парламентаризму. *Віче.* 1997. № 12. С. 28.

12. Теплюк М.О. Парламентський контроль – одна з основних функцій парламенту України: матер. міжнар. наук.-практ. конф. *Парламентаризм в Україні: теорія та практика,* м. Київ, 26 черв. 2001 р. Київ: Ін-т законодавства Верховної Ради України, 2001. С. 463-468.

13. Майданник О.О. Теоретичні проблеми контрольної функції парламенту України: автореф. дис. …д-ра юрид. наук. К., 2008. С. 17.

14. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141 (з наступними змінами).

15. Про комітети Верховної Ради України: Закон України від 04.04.95 р. № 116/95-ВР (в редакції від 18.11.2009).

16. Про Регламент Верховної Ради України: Закон України від 10.02.10 р. № 1861-VI (в редакції від 06.04.2010).

17. Рішення Конституційного Суду України у справі за конституційним поданням Президента України щодо відповідності Конституції України (конституційності) положень пункту 4 статті 9, пунктів 4, 5 статті 10, підпункту “г” пункту 1 статті 24, пункту 3 статті 26 Закону України “Про організаційно-правові основи боротьби з організованою злочинністю” від 27.05.09 р. № 12-рп/2009. *Вісник Конституційного Суду України*. 2009. № 4. Стор. 22.

18. Рішення у справі за конституційним поданням 58 народних депутатів України щодо відповідності Конституції України (конституційності) положень пунктів 3, 4, 5, 6 статті 9, пунктів 3, 4, 5 статті 10, підпункту “г” пункту 1 статті 24, пункту 3 статті 26 Закону України “Про організаційно-правові основи боротьби з організованою злочинністю”, пункту 10 статті 14, статті 33-1 Закону України “Про комітети Верховної Ради України” від 10.06.10 р. № 16-рп/2010. *Офіційний вісник України*. 2010 р. № 49. Стор. 221. Ст. 1611.

19. Постанова Вищого адміністративного суду України від 4 грудня 2012 року у справі № К/9991/40827/11.

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

УДК 343.431

ЖИРОВА П.О., *магістр,* Національний університет "Одеська морська академія"

ЗАПОБІГАННЯ ТОРГІВЛІ ЛЮДЬМИ В УКРАЇНІ: МІЖНАРОДНІ СТАНДАРТИ ТА СТАН РЕАЛІЗАЦІЇ

Анотація. *У статті розглядаються результати доктринальних досліджень та поглядів вчених стосовно виконання міжнародних стандартів з запобігання торгівлі людьми в Україні. Запропоновано шляхи покращення реалізації міжнародних стандартів.*

Ключові слова: *торгівля людьми, міжнародні стандарти, стан реалізації.*

Summary. *The results of doctrine researches and views of scientists in relation to implementation of international standards in prevention of people trafficking in Ukraine are examined in the article. The ways of improvement of implementation of international standards are offered.*

Keywords: *people trafficking, international standards, state of realization.*

Аннотация. *В статье рассматриваются результаты доктринальных исследований и взгляды ученых относительно выполнения международных стандартов по предотвращению торговли людьми в Украине. Предложены пути улучшения реализации международных стандартов.*

Ключевые слова: *торговля людьми, международные стандарты, состояние реализации.*

Постановка проблеми. Торгівля людьми на сьогоднішній день є загостреною проблемою для всього світу. Свідченням стурбованості міжнародного співтовариства ситуацією, що склалася, є ряд конвенцій, пактів та протоколів з врегулювання цього питання. Зауважимо, що проблематика торгівлі людьми зазнає змін, що створює у свою чергу складнощі для виявлення постраждалих та надання їм допомоги, ведення профілактичної роботи, а також ефективного розслідування таких справ. Заходи щодо протидії торгівлі людьми повинні будуватися на основі дієвого національного законодавства, що приймається на базі загальноприйнятих міжнародних норм. На жаль в Україні існує проблематика щодо реалізації міжнародних стандартів запобігання торгівлі людьми. У зв'язку з чим вважаємо, що на сьогодні необхідно дослідити стан реалізації міжнародних стандартів щодо запобігання торгівлі людьми в Україні.

Результати аналізу наукових публікацій. Окремі питання щодо запобігання торгівлею людьми в Україні були предметом дослідження таких вчених, як: М.І. Андрієнко, Н.М. Ахтирська, А.Ф. Возний, В.І. Варивода, В.І. Василинчук, Т.І. Возна, А.І. Волкова, В.Ф. Дерюжинський, К.О. Дядюра, О. Ємець, В.О. Іващенко, О.В. Кушнір, К.Б. Левченко, К.І. Левченко, В.В. Максимов, Ю.С. Нагачевська, Д.Й. Никифорчук та ін. Незважаючи на значну кількість наукових розвідок, що присвячені запобіганню торгівлі людьми в Україні, недостатня увага на сьогодні приділена саме дослідженню стану реалізації міжнародних стандартів щодо запобігання торгівлі людьми в Україні.

Метою статті є визначення стану реалізації міжнародних стандартів щодо запобігання торгівлі людьми в Україні

Виклад основного матеріалу. На сьогодні на міжнародному рівні основними міжнародними організаціями, які займаються розробленням і впровадженням міжнародних стандартів щодо запобігання торгівлі людьми є Організація Об'єднаних Націй, Рада Європи, Європейський Союз, Організація з безпеки і співробітництва в Європі (ОБСЄ), міжнародні міжурядові та неурядові організації, такі як, наприклад, Міжнародна Ліга жінок за мир і свободу, Міжнародна Демократична Федерація жінок,

Всесвітня організація за виживання (The Global Survival Network), Фонд проти торгівлі людьми (The Foundation Against Trafficking) та багато інших [1].

Так, до прикладу, Палермська Конвенція ООН і Протокол до неї, прийнятий в листопаді 2000 року, визначає, що торгівля людьми є одним з найбільш небезпечних кримінальних карних діянь [2]. У свою чергу, Конвенція про боротьбу з торгівлею людьми та експлуатацією проституції третіми особами, прийнята Генеральною Асамблеєю ООН від 2 грудня 1949 року, консолідує положення інших міжнародних договорів з цього питання, прийнятих починаючи з 1904 року. Її основне завдання – визначення ефективних мір боротьби проти усіх форм торгівлі жінками та експлуатації проституції. Вперше в історії укладення міжнародних договорів, дана Конвенція проголосила проституцію і торгівлю людьми актами, несумісними з гідністю і цінністю людської особистості, що ставлять під загрозу добробут окремих осіб, сім'ї та суспільства [3]. Міжнародний пакт про громадянські та політичні права 1966 року, який є доповненням до Загальної декларації прав людини, а саме захищає право на життя, встановлює, що жодна людина не повинна піддаватися випробуванням, примусовій праці і незаконному утриманню чи утиску таких свобод як свобода на пересування, вираження та асоціацію з іншими [4].

Важливо розглянути Декларацію європейських рекомендацій з ефективних заходів щодо запобігання боротьби з торгівлею жінками, яка була прийнята в 1997 році. Її ціль – підтримка подальших дій з попередження торгівлі людьми, а також надання необхідної допомоги жертвам торгівлі. Розглядаючи документ про Спільну дію Ради Європи від 1997 року, слід зауважити, що він перелічує додаткові види покарання і заходи адміністративного характеру, такі як конфіскація і вилучення доходів і власності торговця людьми і закриття установ, які брали участь у торгівлі людьми. Також документ зобов'язує країни-члени ЄС ввести адміністративну або кримінальну відповідальність за злочини, вчинені від імені юридичної особи без урахування кримінальної відповідальності фізичних осіб, що стали співучасниками або призвідниками злочину [5].

Нині на рівні ЄС діє Рамкове рішення Ради Європи про торгівлю людьми. Його метою є уніфікація національного кримінального законодавства для забезпечення ефективної боротьби з торгівлею людьми. Воно доповнює вже прийняті Радою Європи інструменти, такі як "Спільні дії" від 1996, 1998 та 2000 рр., а також програми STOP (спрямована головним чином на розроблення міждисциплінарного підходу із залученням усіх зацікавлених сторін і приділяє велику увагу дуже важливій ролі неурядових організацій) та DAPHNE (спеціально розроблена з метою підтримки діяльності неурядових організацій у сфері захисту жінок і дітей – жертв насильства) [6].

Конвенція ООН проти транснаціональної організованої злочинності від 15 листопада 2000 року (Нью Йорк), має за мету сприяння міжнародному співробітництву для запобігання транснаціональній організованій злочинності і боротьбі проти неї. Надає правоохоронним органам і судовій владі унікальні засоби боротьби з цією проблемою [2]. Протокол про попередження і запобігання торгівлі людьми, особливо жінками і дітьми, і покарання за неї є доповненням до вищеназваної Конвенції. Вперше дає міжнародне визначення поняття "торгівля людьми"; слугує для попередження, боротьби і закріплення міжнародного співробітництва в боротьбі проти цього злочину; визначає загальну термінологію, гармонізує закони і практику, що застосовуються в різних країнах. Згідно цьому Протоколу, торгівля людьми – це комплекс дій з рекрутування, транспортування, передачі та отримання осіб з використанням загроз застосування сили, інших форм примусу, залякування, або через надання неправдивих

відомостей щодо можливості отримання (заробітку) грошей у місці призначення. Неодмінним атрибутом торгівлі людьми є отримання контролю над особою (наприклад, через вилучення документів) з метою експлуатації [7].

Зауважимо, що це є не вичерпний перелік міжнародних нормативно-правових актів, які здійснюють правову регламентацію та встановлюють міжнародні стандарти щодо запобігання торгівлі людьми в світі. Слід відзначити, що більшість міжнародних норм які здійснюють правове регулювання щодо запобігання торгівлі людьми, є частиною національного законодавства України. Це великий крок для нашої країни на шляху встановлення міжнародних стандартів щодо протидії торгівлі людьми.

Також, вважаємо за необхідність в межах даного дослідження розглянути досвід Федеративної Республіки Німеччина щодо запобігання торгівлі людьми. Безпосередньо для нас цікавою є наявність загальнонаціональної Робочої групи з питань боротьби з торгівлею жінками (створеної 1997 року з метою успішнішої протидії торгівлі жінками Федеральним міністерством у справах сім'ї, осіб похилого віку, жінок та молоді), у роботі якої беруть участь представники різних федеральних та земельних міністерств, Федеральна служба кримінальної поліції, а також інші заінтересовані структури. До завдань Робочої групи належить: обмін інформацією щодо заходів по боротьбі з торгівлею жінками; аналіз проблем, які можуть виникнути у ході здійснення заходів з протидії торгівлі жінками; опрацювання спільних пропозицій та планів дій; підготовка заяв від імені Німеччини у контексті міжнародних заходів [8].

Уряд Німеччини обрав протидію торгівлі людьми шляхом мобілізації зусиль правоохоронних органів. Законодавство Німеччини забороняє торгівлю людьми у будь-якій формі; торгівля людьми з метою сексуальної експлуатації та примусової праці є злочинами. Покарання за такі злочини передбачає до 10 років позбавлення волі. Водночас урядом Німеччини приділяється значна увага і превентивній роботі, зокрема фінансується діяльність цілої низки неурядових організацій, що проводять інформаційно-освітні кампанії з попередження торгівлі людьми як у самій Німеччині, так і за її межами [8]. Нині у Німеччині використовується чотири стандартні бази даних, у яких міститься інформація щодо фактів торгівлі людьми: статистика злочинів, куди вносяться дані поліцейських розслідувань; звіти щодо ситуації у зв'язку з існуванням явища торгівлі людьми, які складаються Федеральним бюро кримінальних розслідувань Німеччини; статистика по справах, що передані до суду; центральний реєстр кримінальних справ, що містить інформацію стосовно розглядів. Також слід погодитись із Кушнір О.В., яка вказує, що здійснення такої чіткої фіксації усієї інформації у сфері протидії торгівлі людьми дає змогу не лише швидко знаходити потрібну інформацію, а й усунути безліч зайвих дій, що здійснюються працівниками правоохоронних органів нашої держави у пошуку прецедентних кримінальних справ, осіб, причетних до скоєння таких злочинів, а також розгляду зазначеної категорії справ у судах. Крім того, чітко окреслюється і ситуація з розгляду кримінальних справ у судах, кількості осіб, притягнутих до відповідальності (для України створення таких баз даних є конче необхідним, оскільки дуже багато справ у суді роками "припадають пилом", їх розгляд затягується, а вироки не відповідають реальному ступеню завданої злочином шкоди та наслідків, і відслідкувати реальну ситуацію стає дуже складно, бо одні працівники змінюються на інших, дані втрачаються і в результаті відбувається "запізнення отримання" та "мішанина" інформації). До того ж існування таких баз суттєво спрощує процедуру пошуку й фіксації речових доказів та в цілому підвищує рівень можливостей у протидії торгівлі людьми [8].

Що стосується безпосередньо стану реалізації міжнародних стандартів запобігання торгівлі людьми в Україні, слід зауважити, що наша держава є учасником міжнародних актів щодо співпраці та запобігання торгівлі людьми. Як зазначає О. Ємець, криміналізація торгівлі людьми в Україні відбулась у 1998 році, а з прийняттям 2001 року нового Кримінального кодексу відповідальність за такі дії передбачена ст. 149. Проте ця стаття мала суттєві недоліки, зокрема її диспозиція передбачала обов'язкове переміщення через державний кордон потерпілої особи. В 2006 році приймається нова редакція цієї статті, яка більше відповідає реаліям сьогодення. Диспозиція статті передбачає кримінальну відповідальність за торгівлю людьми або здійснення іншої незаконної угоди, об'єктом якої є людина, а так само вербування, переміщення, переховування, передачу або одержання людини, вчинені з метою експлуатації, з використанням обману, шантажу чи уразливого стану особи. Незважаючи на позитивні зміни, і в такому вигляді стаття має певні вади. Еволюція формулювання кримінально-правової норми свідчить про бажання її удосконалити та підтверджує намір дотриматись зобов'язань щодо імплементації положень міжнародних актів у національне законодавство. Критика цієї оновленої редакції статті не припиняється, зокрема вказується на те, що нова стаття виявилась не бездоганною з точки зору юридичної техніки, що породжуватиме певні проблеми при її застосуванні. Є необхідність розширеного тлумачення таких понять, як "вербування", "переміщення", "шантаж", "уразливий стан особи", "переховування", "передача або одержання людини" з метою їх єдиного трактування та застосування правоохоронними органами. Роз'яснення таких понять з їх розмежуванням може подаватися в примітці до статті, а за відсутності такого – у постановах пленуму Верховного Суду України [9, с. 186-187].

Крім того, прийняття Україною у вересні 2011 року Закону "Про протидію торгівлі людьми" суттєво наблизило українське законодавство до найкращих міжнародних стандартів в цій сфері. Відтак, українське законодавство в цілому відповідає положенням Конвенції Ради Європи про заходи щодо протидії торгівлі людьми (стаття 149 Кримінального Кодексу України, Закон України "Про протидію торгівлі людьми"). В Україні передбачено достатньо суворі та адекватні санкції за торгівлю людьми та пов'язані з нею злочини. У законі "Про протидію торгівлі людьми" міститься низка інноваційних положень, які стосуються захисту потерпілих від торгівлі людьми. Наприклад, з метою ефективної допомоги особам, які постраждали від торгівлі людьми, та їх захисту створюється Національний механізм взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми [10]. Закон України "Про протидію торгівлі людьми" визначає, що боротьба з торгівлею людьми – система заходів, що здійснюються в рамках протидії торгівлі людьми, спрямованих на виявлення злочину торгівлі людьми, у тому числі незакінченого, осіб, які від цього постраждали, встановлення фізичних/юридичних осіб – торгівців людьми та притягнення їх до відповідальності [11].

На виконання Закону України "Про протидію торгівлі людьми" було прийнято Постанову КМУ "Про затвердження Державної цільової соціальної програми протидії торгівлі людьми на період до 2015 року" яка передбачає, що метою Програми є запобігання торгівлі людьми, підвищення ефективності переслідування осіб, які вчиняють пов'язані з нею злочини або сприяють їх вчиненню, а також захист прав осіб, що постраждали від торгівлі людьми, та надання їм допомоги [12]. В Постанові зазначається, що можливі два варіанти розв'язання проблеми торгівлі людьми та надання допомоги і захисту особам, що постраждали від неї. Перший варіант полягає у розв'язанні проблеми торгівлі людьми шляхом здійснення системних заходів державними установами за рахунок бюджетних коштів. Недоліком зазначеного варіанта

є те, що для його реалізації необхідні бюджетні кошти у значному обсязі. Другий, оптимальний варіант передбачає налагодження співпраці державних установ з громадськими організаціями, зокрема впровадження ефективного механізму взаємодії у сфері протидії торгівлі людьми, за такими напрямами, як: організація інформаційно-роз'яснювальної роботи серед населення, спрямованої на запобігання потраплянню в ситуації, пов'язані з торгівлею людьми; підвищення професійного рівня спеціалістів, які надають допомогу особам, що постраждали від торгівлі людьми, здійснюють їх реабілітацію та соціальну реінтеграцію; проведення постійного моніторингу ефективності заходів, спрямованих на протидію торгівлі людьми; підвищення якості надання послуг особам, що постраждали від торгівлі людьми, зокрема шляхом впровадження стандартів надання соціальних послуг таким особам. Незважаючи на наявність законодавства, що передбачає протидію торгівлі людьми, проблемні аспекти правового регулювання не вичерпано [12].

Зокрема, згідно Дослідження Української Гельсінської спілки з прав людини до основних організаційно-правових проблем порушення прав осіб, які страждають від торгівлі людьми, відносяться наступні:

1) стаття 17 Закону України "Про протидію торгівлі людьми" визначає, що для забезпечення реалізації прав, передбачених Законом, особи, які постраждали від торгівлі людьми, можуть бути направлені до одного з центрів соціальних служб для сім'ї, дітей та молоді, центрів соціального обслуговування (надання соціальних послуг) або до центрів соціально-психологічної реабілітації дітей та притулків для дітей, у випадку, коли постраждала особа є неповнолітньою [11]. Проте, відповідно до положень зазначених закладів, розроблених на підставі Постанови КМ України від 28 січня 2004 р. № 87 [13], а також Постанови КМ України від 29 грудня 2009 р. № 1417 [14], така категорія осіб, як постраждалі від торгівлі людьми, не включена до переліку осіб, які мають право на отримання послуг у цих закладах. Крім того, існують складнощі з ідентифікацією постраждалих від торгівлі людьми серед загальної кількості клієнтів (осіб, які перебувають у складних життєвих обставинах) зазначених закладів. Залишається проблемним питання надання допомоги постраждалим особам з інших країн, забезпечення їхніх потреб у захисті та допомозі під час перебування в Україні;

2) відсутність в Законі та відповідних підзаконних актах положення про встановлення періоду реабілітації та обмірковування для осіб, відносно яких є підстави вважати, що вони постраждали від торгівлі людьми, також призводить до порушення прав постраждалих, особливо громадян інших країн. Вважається за доцільне внести зазначені положення, які містяться в ключових міжнародних документах, до національних нормативних актів, врахувавши наявний досвід інших країн, де період реабілітації та обмірковування є вже сталою нормою;

3) незважаючи на наявність в Законі України "Про протидію торгівлі людьми" положень щодо необхідності оцінки ризиків повернення постраждалої особи до країни походження (ст. 16 "Права особи, яка постраждала від торгівлі людьми" та ст. 24 "Повернення або залишення дитини, яка постраждала від торгівлі дітьми"), нормативні документи, що були прийняті на виконання закону, не містять чіткої процедури проведення оцінки таких ризиків. Також дана процедура не включена в положення, якими керуються в своїй діяльності суб'єкти, які здійснюють заходи у сфері протидії торгівлі людьми;

4) мають місце складнощі та порушення і під час процесу відшкодування потерпілим майнової, моральної та фізичної шкоди, якої вони зазнали внаслідок вчинення злочину торгівля людьми. Серед них: формальний підхід слідчих до роз'яснення потерпілим їхніх

прав заявити позов про компенсацію; необхідність довести факт моральних страждань; віддаленість експертних центрів та нечисленність атестованих судових експертів-психологів; відсутність практики міжнародного співробітництва щодо захисту майнових прав громадян України; недосконалий законодавчий механізм стягнення компенсації; недієвість ст. 1177 Цивільного кодексу України щодо зобов'язань держави відшкодовувати збитки потерпілим тощо;

5) досі не були прийняті стандарти щодо здійснення послуг у сфери протидії торгівлі людьми, які були розроблені та подані до Міністерства соціальної політики групою експертів – представників державних, неурядових та міжнародних організацій ще в 2010 р. [15].

Висновки.

На основі проведеного дослідження, слід зазначити, що на сьогодні в нашій країні існує необхідність нормотворчої діяльності для забезпечення практичної реалізації міжнародних стандартів щодо запобігання торгівлею людьми. Нагальною є потреба у створенні ефективних механізмів державного управління міграційними процесами, які б сприяли запровадженню дієвих заходів з протидії нелегальній міграції та торгівлі людьми. Важливою складовою цього процесу є використання європейського досвіду державного управління з протидії незаконній міграції та торгівлі людьми зокрема.

Перспективи подальших досліджень. Вважаємо, що необхідно проаналізувати досвід Федеративної Республіки Німеччина та створити робочу групу з питань боротьби з торгівлею людьми, а також здійснити ряд інформаційно-організаційних заходів щодо створення належної бази даних на прикладі Німеччини, яка буде містити інформацію щодо фактів торгівлі людьми.

Використана література

1. Подшивалов В.Е. Незаконная миграция: международно-правовой поход. *Правоведение.* 2002. № 4. С. 63-65.

2. Про транснаціональну злочинність: Конвенція ООН від 15 листопада 2000 р. URL: http://zakon.rada.gov.ua/laws/show/995_789

3. Про боротьбу з торгівлею людьми та експлуатацією проституції третіми особами: Конвенція ООН від 2 грудня 1949 р. URL: http://zakon.rada.gov.ua/laws/show/ 995_162

4. Міжнародний пакт про громадянські та політичні права: Пакт ООН від 16 грудня 1966 р. URL: http://zakon.rada.gov.ua/laws/show/995_043

5. Декларація європейських рекомендацій з ефективних заходів щодо запобігання боротьби з торгівлею жінкам: Рекомендації Ради Європи від 24 квітня 1997 р. URL: http://lib.rada.gov.ua/DocDescription?doc_id=13034

6. Дядюра К.О. Засоби протидії торгівлі людьми: міжнародно-правовий досвід. URL: http://www.pravoznavec.com.ua/period/article/59688/%CA

7. О предупреждении и пресечении торговли людьми, особенно женщинами и детьми, и наказании за нее: Резолюция ООН от 15 ноября 2000 г. № 55/25 (Протокол дополняющий Конвенцию ООН против транснациональной организованной преступности). URL: http://www.un.org/russian

8. URL: http://www.no2slavery.ru/ru/issledovaniya

9. Ємець О. Нормативно-правове забезпечення протидії торгівлі людьми в Україні. *Вісник Академії управління МВС*. 2010. № 4(16). С. 186-192.

10. Наскільки законодавство України у сфері протидії торгівлі людьми відповідає міжнародним стандартам? URL: http://www.lastrada.org.ua/ucp_mod_news_list_ show_274.html

11. Про протидію торгівлі людьми: Закон України. *Відомості Верховної Ради України*. 2012. № 19-20. Ст. 173. URL: http://zakon.rada.gov.ua/laws/show/3739-17

12. Про затвердження Державної цільової соціальної програми протидії торгівлі людьми на період до 2015 року: Постанова Кабінету Міністрів України. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/KP120350.html

13. Про затвердження Типового положення про центр соціально-психологічної реабілітації дітей: Постанова Кабінету Міністрів України від 28.01.04 р. № 87. URL: http://zakon.rada.gov.ua/laws/show/87-2004-%D0%BF

14. Деякі питання діяльності територіальних центрів соціального обслуговування (надання соціальних послуг): Постанова Кабінету Міністрів України від 29.12.09 р. № 1417. URL: http://zakon.rada.gov.ua/laws/show/1417-2009-%D0%BF

15. Торгівля людьми як порушення прав людини. URL: http://helsinki.org.ua/index.php?id=1362662821

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

До відома читачів

ПЕРЕЛІК СТАТЕЙ,

опублікованих у журналі ІНФОРМАЦІЯ І ПРАВО у 2018 р.

№ з/п	Назва статті	Автор(и)	№ журналу, стор.
Інформаційне право			
1	Соціологічний та аксіологічний напрямки сучасних правових досліджень: загальне бачення	Дзьобань О.П., Яроцький В.Л.	1(24)/2018, с. 5-13
2	Вільний доступ громадян до правової інформації – засаднича ознака забезпечення правової безпеки держави	Корж І.Ф.	1(24)/2018, с. 14-27
3	Вплив загального регулювання захисту даних на контролерів та процесорів персональних даних – резидентів України	Тарасюк А.В.	1(24)/2018, с. 28-35
4	Дистанційне зондування Землі: минуле і сучасне міжнародно-правового регулювання отримання і використання інформації	Забара І.М.	1(24)/2018, с. 36-43
5	Веб-сайти органів державної влади та органів місцевого самоврядування: механізми доступу до публічної інформації	Корж І.Ф.	2(25)/2018, с. 9-16
6	Інформаційні права і свободи людини і громадянина в Україні: визначення термінів, співвідношення понять	Ткачук Н.І.	2(25)/2018, с. 17-30
7	Фактори, що впливають на утворення системи інформаційного права та формування її змісту	Панова І.В.	3(26)/2018, с. 9-15
8	Правовий захист та безпека персональних даних: соціальний та комерційний аспекти	Брижко В.М.	3(26)/2018, с. 16-37
9	Міжнародно-правове регулювання використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій: до двадцятиріччя конвенції тампере 1998 року	Забара І.М.	3(26)/2018, с. 38-48
10	Інформаційні ресурси як елемент національної інформаційної інфраструктури: їх створення та використання	Чорноус А.Г.	3(26)/2018, с. 49-55
11	Децентралізація та її вплив на розвиток регіональних суспільних відносин	Корж І.Ф.	4(27)/2018, с. 9-14
12	Зміст поняття “державні електронні інформаційні ресурси”	Марущак А.І., Петров С.Г.	4(27)/2018, с. 15-21
13	Заборона використання сили у кіберпросторі за міжнародним правом	Яцишин М.Ю.	4(27)/2018, с. 22-32
14	Виклики і загрози правам та безпеці людини в інформаційній сфері	Уханова Н.С.	4(27)/2018, с. 33-45
Правова інформатика			
15	Інструменти державного стратегічного управління: Національна програма інформатизації	Жиляєв І.Б., Семенченко А.І., Фурашев В.М.	1(24)/2018, с. 44-58
16	Інтернет речей (IoT) і блокчейн	Баранов О.А.	1(24)/2018, с. 59-71
17	Компрометація особистого ключа електронного підпису: правовий аспект	Костенко О.В.	1(24)/2018, с. 72-80

18	Розвиток правової кібернетики у Польщі в XX-му сторіччі	Рафал Канія (Rafał Kania)	1(24)/2018, с. 81-89
19	Інтернет речей (IoT): мета застосування та правові проблеми	Баранов О.А.	2(25)/2018, с. 31-44
20	Досвід Ізраїлю у сфері забезпечення кібербезпеки	Леонов Б.Д., Лук'янчук Р.В.	2(25)/2018, с. 45-50
21	Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності	Довгань О.Д., Тарасюк А.В.	2(25)/2018, с. 51-61
22	Розвиток електронного парламентаризму як ознака подальшої демократизації держави	Корж І.Ф.	3(26)/2018, с. 56-67
23	Система анотування китайської правової інформації	Ланде Д.В., Яньцін Чжао, Моцзі Вей, Шівей Чжу, Цзяньпін Го.	3(26)/2018, с. 68-75
24	Електронний підпис та електронні довірчі послуги в законодавстві Сполучених Штатів Америки	Костенко О.В.	3(26)/2018, с. 76-84
25	Інтернет речей (IoT): регулювання надання послуг роботами з штучним інтелектом	Баранов О.А.	4(27)/2018, с. 46-70
26	Узагальнення індексу цитування як компенсація неповноти наукометричних база даних	Брайчевський С.М	4(27)/2018, с. 71-78
Інформаційна і національна безпека			
27	Система інформаційної безпеки України: онтологічні виміри	Довгань О.Д., Ткачук Т.Ю.	1(24)/2018, с. 89-103
28	Трансформація національної безпеки в інформаційну епоху: загальна доктрина та її правова складова	Доронін І.М.	1(24)/2018, с. 104-111
29	Реформування системи охорони державної таємниці: правові аспекти	Болдир С.В.	1(24)/2018, с. 112-120
30	Застосування сучасних технологій і методів виявлення та розпізнавання осіб, які мають вчинити теракт	Парфило О.А., Леонов Б.Д.	1(24)/2018, с. 121-126
31	Інформаційно-правові аспекти протидії кіберзлочинності	Марущак А.І.	1(24)/2018, с. 127-132
32	Організаційно-правові засади формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави	Ткачук Н.А.	1(24)/2018 с. 133-138
33	Ґенеза суспільних відносин щодо інформаційної безпеки людини	Золотар О.О.	1(24)/2018, с. 139-148
34	Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності	Довгань О.Д., Тарасюк А.В.	2(25)/2018, с. 51-61
35	Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні	Пилипчук В.Г., Доронин І.М.	2(25)/2018, с. 62-72
36	Правове забезпечення інформаційної безпеки держави як підгалузь інформаційного права: теоретичний дискурс	Довгань О.Д., Ткачук Т.Ю.	2(25)/2018, с. 73-85
37	Екстраординарний характер реалізації безпекових функцій держави в сучасному світі: інформаційно-правовий аспект	Доронін І.М.	2(25)/2018, с. 86-95
38	Тенденції розвитку медіа-сфери України у контексті інформаційної безпеки України	Марущак А.І.	2(25)/2018, с. 96-102
39	Правове регулювання міжнародних міграційних процесів	Бєлєвцева В.В.	2(25)/2018, с. 103-109
40	Правові засоби забезпечення національної міграційної безпеки України	Денисов А.І.	2(25)/2018, с. 110-116

41	Нормативно-правове забезпечення в Україні питання утримання та поводження з військовополоненими та інтернованими особами в особливий період	Блистів Т.І.	2(25)/2018, с. 117-123
42	Протидія антидержавному екстремізму як інструменту обмеження державного суверенітету в сучасних умовах	Кучерина С.Є., Олєйніков Д.О.	2(25)/2018, с. 124-133
43	Протидія негативним інформаційним впливам на людину і суспільство в умовах гібридної війни.	Мосов С.П., Уханова Н.С.	2(25)/2018, с. 134-141
44	Поняття та ознаки права національної безпеки України	Богуцький П.П.	3(26)/2018, с. 84-93
45	Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні	Довгань О.Д., Тарасюк А.В.	3(26)/2018, с. 94-103
46	Міжнародне співробітництво у боротьбі з транснаціональною кіберзлочинністю	Марущак А.І.	3(26)/2018, с. 104-110
47	Протидія використанню учасниками злочинних угруповань мережі “Даркнет”	Гуцалюк М.В.	3(26)/2018, с. 11-117
48	Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права	Довгань О.Д., Ткачук Т.Ю.	4(27)/2018, с. 79-89
49	Оборонні “Білі книги”: правові аспекти інформування суспільства про діяльність сектору безпеки і оборони у контексті громадського контролю	Доронін І.М.	4(27)/2018, с. 90-97
50	Захист від недобросовісної конкуренції: нормативно-правовий та інформаційний аспекти	Євтушенко Є.В Леонов Б.Д.	4(27)/2018, с. 98-103
51	Правове регулювання взаємодії Служби безпеки України з приватним сектором у сфері забезпечення кібербезпеки	Ткачук Н.А.	4(27)/2018, с. 104-111
52	Діяльність військової контррозвідки в Армії США: організаційно-правовий аспект	Кравченко Р.М.	4(27)/2018, с. 112-120
53	Основні підходи до визначення поняття “біотероризм”	Квасюк В.В.	4(27)/2018, с. 121-125
54	Інформаційне-правове забезпечення спеціальних інформаційних операцій	Верголяс О.О.	4(27)/2018, с. 126-133
Інформація за іншими предметними напрямами досліджень за спеціалізаціями в галузі знань 08 – “Право”			
55	Штучній інтелект, інформаційна безпека та законотворчий процес (кримінально-правовий аспект)	Радутний О.Е.	1(24)/2018, с. 149-158
56	Соціально-демографічні ознаки осіб, які вчинили сімейне насильство щодо дітей	Беспаль О.Л.	1(24)/2018, с. 159-163
57	Інформаційні правовідносини в контексті цивільного судочинства	Солончук І.В.	1(24)/2018, с. 164-173
58	Інформаційний інструментарій розколу української політичної еміграції у міжвоєнний період: незасвоєні уроки минулого	Вронська Т.В.	2(25)/2018, с. 142-157
59	Цифрова людина з точки зору загальної та інформаційної безпеки: філософський та кримінально-правовий аспект	Радутний О.Е.	2(25)/2018, с. 158-170
60	Деякі чинники, які впливають на суспільні відносини та закладають основи їх формування в майбутньому	Юдкова К.В.	2(25)/2018, с. 170-176
61	Кримінально-правові проблеми трансплантології в Україні: шляхи їх вирішення та перспективи розвитку	Барсученко Ю.О	2(25)/2018, с. 177-182
62	Регулювання та нагляд в фінансовій сфері: модель “Твін пікс”	Вишневський Є.І.	3(26)/2018, с. 118-130

63	Забезпечення права на справедливий суд: міжнародне закріплення та вітчизняні здобутки	Романів Х.Б.	3(26)/2018, с. 131-136
64	Сучасні тенденції надання комітетам Верховної Ради України спеціальних повноважень для здійснення парламентського контролю: організаційно-правовий аспект	Нижник А.І.	4(27)/2018, с. 134-142
65	Запобігання торгівлі людьми в Україні: міжнародні стандарти та стан реалізації	Жирова П.О.	4(27)/2018, с. 143-149

До відома читачів

Нове наукове видання: ***Становлення і розвиток правових основ та системи захисту персональних даних в Україні*****:** монографія……..……	1(24)/2018, с. 174
Нове видання: ***Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних*****:** зб. перекл. документів…...	3(26)/2018, с. 137
Перелік статей, опублікованих у журналі ІНФОРМАЦІЯ І ПРАВО у 2017 р. ….	1(24)/2018, с. 175-177

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

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. (або за рішенням редакції).*

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)* та **результати аналізу наукових публікацій**, в яких започатковано розв'язання проблеми, виділення не вирішених її частин, котрим присвячується стаття; **наводяться аргументи які 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 використаних джерел 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(27)/2018

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.