

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

№ 2(33)/2020

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

Згідно з Наказом МОН України від 02.07.20 р. № 886 (додаток 4) журнал включено до Переліку наукових фахових видань України, категорія “Б”, галузь науки - юридичні, спеціальність - 081. 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, розміщується на інформаційній платформі “Наукова періодика України”, через яку здійснюється інтеграція з регіональним Реєстром DOI, Системою CrossRef, Міжнародним реєстром ORCID.

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

№ 2(33)/2020

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

Pursuant to Order of the Ministry of Education and Science of Ukraine dated 02.07.20 № 886 (Annex 4), the journal is included in the List of scientific professional publications of Ukraine, category “B”, branch of science - legal, specialty - 081.

The journal can publish materials related to thesis works aimed on the receipt of scientific degrees of Doctor of Philosophy – Ph.D. (candidate of sciences) 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, is placed on the information platform “Scientific Periodicals of Ukraine”, through which integration with the regional DOI Register, CrossRef System, ORCID International Register is carried out.

Kyiv

УДК 002:340+316.4+338.46

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

* * * * *

UDC 002:340+316.4+338.46

THE SCIENTIFIC COUNCIL OF THE JOURNAL

Pylypchuk Volodymyr, Doctor of Juridical Science, Professor, Corresponding Member NALS of Ukraine – *Chairman of Editorial Board*.

Dubrovina Lyubov, Doctor of Historical Sciences, Professor, Corresponding Member National Academy of Sciences of Ukraine – *Vice-chairman of Editorial Board*.

Bebyk Valerii, Doctor of Political Sciences, Professor – *Vice-chairman of Editorial Board*.

Kuibida Vasyl, Doctor of Administration Science, Professor.

Kopan Oleksii, Doctor of Juridical Science, Professor.

Marushchak Anatolii, Doctor of Juridical Science, Professor

Nor Vasyl, Doctor of Juridical Science, Professor, Academician NALS of Ukraine.

Onishchenko Oleksii, Doctor of Philosophical Science, Professor, Academician NAN of Ukraine.

Petryshin Oleksandr, Doctor of Juridical Science, Professor, Academician NALS of Ukraine.

Pokutnyi Serhii, Doctor of Physics and Mathematics Sciences, Professor.

Savinova Nataliia, Doctor of Juridical Science, Senior researcher fellow.

Skulysh Ievhen, Doctor of Juridical Science, Professor.

Talanchuk Petro, Doctor of Engineering Sciences, Professor.

Tykhyy Volodymyr, Doctor of Juridical Science, Professor, Academician NALS of Ukraine.

Furashev Volodymyr, Candidate of Engineering Sciences, Associate Professor,
Senior researcher fellow.

Shemshuchenko Yurii, Doctor of Juridical Science, Professor, Academician NAN of Ukraine.

EDITORIAL BOARD

Bukhanevych Oleksandr, Doctor of Juridical Science, Professor – *Editor in Chief*.

Dovgan Oleksandr, Doctor of Juridical Science, Professor – *Vice-Editor*.

Bryzhko Valerii, Doctor of Philosophy of Juridical Science, Senior researcher fellow
– *Vice-Editor*.

Tomasz Schaffler, Doctor of Philosophy of Juridical Science (University of Wroclaw, Poland).

Waldemar Bednaruk, Doctor habilitowany (Catholic University of Lublin, Poland).

Aristova Iryna, Doctor of Juridical Science, Professor.

Baranov Oleksandr, Doctor of Juridical Science, Senior researcher fellow.

Bieliakov Konstantyn, Doctor of Juridical Science, Professor.

Chistokletov Leontiy, Doctor of Juridical Science, Professor.

Dz'oban Oleksandr, Doctor of Philosophical Science, Professor.

Doronin Ivan, Candidate of Juridical Science, Associate Professor.

Zolotar Olga, Doctor of Juridical Science, Senior researcher fellow.

Korzh Ihor, Doctor of Juridical Science, Senior researcher fellow.

Lande Dmytro, Doctor of Engineering Sciences, Professor.

Nastiuk Vasyl, Doctor of Juridical Science, Professor, Corresponding Member NALS of Ukraine.

Shevchuk Oleksandr, Doctor of Juridical Science, Associate Professor.

Tkachuk Taras, Doctor of Juridical Science, Associate Professor.

Vronska Tamara, Doctor of Historical Science, Senior researcher fellow.

* * * * *

З М І С Т

Інформаційне право

ДЗЬОБАНЬ О.П., ЖДАНЕНКО С.Б. Права людини і національна безпека: філософсько-правові аспекти взаємозв'язку.....	9
КОСІЛОВА О.І. Тлумачення статті 21 Конституції України у контексті європейської правової доктрини.....	23
ЛЕОНОВ Б.Д., ЧУМАК Л.А., ГРИНЕНКО С.В. Проблеми запобігання сексуальній експлуатації дітей в мережі Інтернет: досвід ЄС.....	32
УХАНОВА Н.С. Особливості захисту прав неповнолітніх в інформаційному просторі.....	40

Правова інформатика

ЛАНДЕ Д.В. Правові питання конкурентної розвідки.....	51
БРАЙЧЕВСЬКИЙ С.М. Проблема персональних даних при використанні систем Інтернету речей в галузі охорони здоров'я.....	69

Інформаційна і національна безпека

МАРУЩАК А.І., ПЕТРОВ С.Г. Сучасний стан розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'язку України). ..	77
ДОВГАНЬ О.Д., ТАРАСЮК А.В. Протидія загрозам кібербезпеці держави на глобальному рівні.....	85
ХАХАНОВСЬКИЙ В.Г., ГАВЛОВСЬКИЙ В.Д. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів.....	99
СТРЕЛЬБИЦЬКА Л.М., СТРЕЛЬБИЦЬКИЙ М.П. Методологічні та організаційно-правові засади формування і функціонування системи державного управління національною безпекою України.....	110
БАТИРГАРЕЄВА В.С. Основні напрями протидії поширенню дезінформації (на прикладі пандемії CoVID-19).....	121
МАЄВСЬКИЙ О.О. Формування інформаційного простору в так званих “ДНР” та “ЛНР” методами експлуатації візуальних образів Другої світової війни.....	132

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

ЯЩЕНКО В.А. Військове право: теоретико-методологічні засади.....	141
КОРЖ І.Ф. Трансформація суспільних відносин у процесі утворення об'єднаних територіальних громад.....	149

ПЕТРИШИН О.О. Реформа місцевого самоврядування: досвід Латвії.....	158
ГОЛОВКО О.М., ДУБЕНЕЦЬ А.С. Роль цифровізації державних послуг у правовідносинах з іноземним елементом.....	170
ВРОНСЬКА Т.В., БЕЛАНЮК М.В. Особливості кримінальної відповідальності цивільного населення в умовах воєнного/надзвичайного стану (на українських землях XVII – початок XX ст.).....	177
До відома авторів.....	194

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

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

Формат 70 x 108/16. Спосіб друку – різнографія. Ум. друк. арк. 17.2. Тираж 100 прим.

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

04050, м. Київ, вул. Мельникова, буд. 63. Свідectво про внесення суб’єкта видавничої справи до
державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції

– серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІП НАПрН України, протокол № 6 від 03.07.20 р.

TABLE OF CONTENTS

Informative Law

DZOBAN O., ZHDANENKO S. Human rights and national security: philosophical and legal aspects of the relationship.....	9
COSILOVA O. Interpretations of Article 21 of the Constitutions of Ukraine in the context of European Legal Doctrine.....	23
LEONOV B., CHUMAK L., GRYNENKO S. The problems of combating the sexual exploitation of children on the internet: analysis of the EU experience.....	32
YKHANOVA N. Features of protection of minors' rights in the information space.....	40

Legal Informatics

LANDE D. Legal issues of competitive intelligence.....	51
BRAYCHEVSKYY S. The problem of personal data when using Internet of Things systems in the field of healthcare.....	69

Informative and National Safety

MARUSHCHAK A., PETROV S. The current development of the National Cybersecurity System (on the example of the Security Service of Ukraine and the State Special Communication Service of Ukraine).	77
DOVGAN O., TARASYUK A. Combating cyber security threats on a global level.....	85
KHAKHANOVSKYI V., GAVLOVSKYI V. Interpretation and classification of criminal offenses as cybercrimes.....	99
STRELBITSKA L., STRELBITSKI M. Methodological and organizational and legal bases of formation and functioning of the system of state management of national security of Ukraine.....	110
BATIRGAREEVA V. Main directions of countering the dissemination of disinformation (on the example of the CoVID-19 pandemic).....	121
MAEVSCI O. Formation of information space in the so-called “DNR” and “LNR” by application of methods of the exploitation of visual images of the Second world war.....	132

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

IASHCHENKO V. Military law: theoretical and methodological principles.....	141
KORZH I. Transformation of social relations in the process of formation of united territorial communities.....	149

PETRYSHIN O. Local government reform: the experience of Latvia.....	158
GOLOVKO O., DUBENETS A. The role of digitization of public services in the legal relationship with a foreign element.....	170
VRONSKA T., BELANYK M. Peculiarities of criminal responsibility of civilian population in conditions of martial law/emergency (in the Ukrainian lands of the 17th – early 20th centuries).....	177
For the consideration of authors	194

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 6 dated 03.07.20

Інформаційне право

УДК 316(477)

ДЗЬОБАНЬ О.П., доктор філософських наук, професор,
головний науковий співробітник НДІП НАПрН України.
ЖДАНЕНКО С.Б., кандидат філософських наук, доцент, доцент кафедри філософії
Національного юридичного університету імені Ярослава Мудрого.

ПРАВА ЛЮДИНИ І НАЦІОНАЛЬНА БЕЗПЕКА: ФІЛОСОФСЬКО-ПРАВОВІ АСПЕКТИ ВЗАЄМОЗВ'ЯЗКУ

Анотація. У статті показано, що права людини і національна безпека тісно взаємопов'язані, причому, реальна взаємозумовленість феноменів національної безпеки і прав людини здебільшого носить суперечливий характер. При цьому проблема взаємозалежності національної безпеки і прав людини є проблемою компромісу між забезпеченням національної безпеки й дотриманням прав людини, між реалізацією прав людини і захистом національної безпеки.

Ключові слова: права людини, національна безпека.

Summary. The article shows that human rights and national security are closely interlinked, and a real interaction of national security and human rights is often controversial. The problem of interdependence of national security and human rights is a problem of compromise between national security and human rights, between human rights implementation and protection of national security.

Keywords: human rights, national security.

Аннотация. В статье показано, что права человека и национальная безопасность тесно взаимосвязаны, причем, реальное взаимообусловленность национальной безопасности и прав человека носит зачастую противоречивый характер. При этом проблема взаимозависимости национальной безопасности и прав человека является проблемой компромисса между обеспечением национальной безопасности и соблюдением прав человека, между реализацией прав человека и защитой национальной безопасности.

Ключевые слова: права человека, национальная безопасность.

Постановка проблеми. На сучасному етапі розвитку цивілізації проблема безпеки для усіх без винятку країн стає однією з найпріоритетніших. Як справедливо зазначає у даному контексті В. Крутов "...наш звичний, більш-менш благополучний післявоєнний світ не раз балансував на межі катастрофи, в тому числі ядерної, від якої його вдавалося врятувати. Але виявилось, що і без ядерних бомб наша планета розколюється як горіх і стає все більш уразливою, руйнуючи сталі уявлення про демократію, свободу, забезпечення прав людини і громадянина, її безпеки тощо" [1, с. 191].

Забезпечення безпеки особистості, суспільства і держави, сьогодні є найважливішою метою реформування країни. При цьому показником політичної стабільності суспільства й держави все частіше виступає рівень реальної захищеності соціально-економічних, цивільних і політичних прав і свобод особистості. Визнання і закріплення на конституційному рівні основних прав, свобод людини і громадянина, постійне розширення їх обсягу та чіткості формулювання їх змісту, гарантій їх реалізації також, поряд з проблемою забезпечення безпеки, є однією з найактуальніших і пріоритетних проблем сучасної цивілізації. Саме тому права людини є тим нормативним

і інституційним контекстом, у якому здійснюється концептуалізація і практичне забезпечення національної безпеки.

Більше того, проблеми безпеки і прав людини корелюють як у теоретичному плані, так і в плані проявів у суспільно-політичному житті. Так, наприклад, відомий західний дослідник В. Бурк-Вайт сформулював три цілком обґрунтовані гіпотези зв'язку ступеня порушень прав людини з проявами міждержавної агресії, а саме: 1) держави, які систематично порушують права і свободи своїх громадян, швидше за все, братимуть участь у міжнародній агресії; 2) держави, в яких права і свободи людини і громадянина захищені посередньо або добре, навряд чи будуть брати участь у міжнародній агресії; 3) держави, в яких поважають права і свободи людини і громадянина, можуть брати участь у міжнародній інтервенції виключно на підставі норм міжнародного права та з метою захисту прав і свобод громадян від порушень з боку власної держави [2].

Отже, права і свободи людини виступають сьогодні одним з найважливіших орієнтирів розвитку концепції національної безпеки. У ході наукових дискусій з питань безпеки прийнято сучасне широке і комплексне розуміння національної безпеки, що складається з трьох елементів – безпеки особистості, суспільства і держави.

Забезпечення безпеки, тобто створення сукупності таких соціально-економічних, політичних, правових та інших умов життєдіяльності, в яких особистість відчувала б себе повністю соціально захищеною, є однією з найважливіших умов існування і розвитку особистості. Стан безпеки особистості – це найважливіший критерій демократичності й цивілізованості сучасного суспільства. Йдеться про прийнятний для особистості соціум, де створені нормально діючі механізми соціального захисту її інтересів, прав і свобод.

Однак реальність насильства й загострення різного роду небезпек і загроз руйнує надії людей на благополучне, безпечне та гідне життя. Здійснюване останнім часом насильство в усіх його проявах стосовно України свідчить про те, що проблема забезпечення безпеки особистості є однією з ключових філософських проблем і повинна лягти в основу вітчизняної політики сталого розвитку.

У сучасних умовах зростає значення безпеки як глобальної цінності людства, зберігається значущість такого її компонента, як гуманітарна безпека, головним об'єктом якої є людина, її інтелектуальний, духовний, морально-етичний потенціал. Людина – це частинка і разом з тим основа будь-якого суспільства і держави. Будь-яка держава має бути зацікавленою у розвитку кожного свого громадянина, в дотриманні безпеки, забезпеченні благ та реалізації інтересів особистості. Незадоволення особистих інтересів громадян неминує призводити суспільство до нестійкого стану, що, у свою чергу, обумовлює такі соціальні явища, як зростання злочинності, страйки, прояви неповаги до держави. Тому, проблема створення сталого суспільства пов'язана з безпекою особистості, з реальними можливостями здійснення її прав і свобод.

Найважливішими факторами, що визначають рівень розвитку суспільства у цілому, а також національну безпеку окремої держави, є такі характеристики, як “свобода людини”, “розвиток людини” і, як наслідок, “забезпечення прав людини”. Це означає, що і гарантією дотримання прав людини є забезпечення безпеки і свобод людини в сучасному розумінні цих слів.

Результати аналізу наукових публікацій з цієї проблеми засвідчили, що дослідники дотримуються різноманітних світоглядних і наукових позицій, і наука поки що не виробила єдиного її розуміння. Одні автори під правами людини розуміють соціальні можливості користування елементарними благами (їжа, одяг, житло, нормальний відпочинок, освіта, недоторканність особи тощо), які існують незалежно від

їх державного визнання. Інші фахівці вважають, що права людини – це соціальні можливості, визнані законом, за порушення яких застосовуються санкції з боку держави. У першому випадку права людини розглядають як соціальну категорію, а у другому – як правову. У той же час, незважаючи на очевидність взаємозв'язку феноменів національної безпеки і прав людини, наукових доробків, присвячених такому їх розгляду, досить мало.

Метою статті є спроба показати, що проблема забезпечення національної безпеки неминуче корелює з проблемою забезпечення прав людини.

Виклад основного матеріалу. У сучасній системі відносин “особистість – держава” є суттєві суперечності. З одного боку, соціальна трансформація і політична модернізація українського суспільства, що почалася ще на початку 1990-х років, поставила на порядок денний якісно нове ставлення держави до особистості, її інтересів, прав і свобод, створення ефективно діючого суспільно-політичного механізму забезпечення безпеки особистості. З іншого боку, особистість усе дедалі більшою мірою стає заручником негативних наслідків економічних, соціально-політичних, науково-технічних та інших технологій суспільного розвитку, способів перетворення суспільного життя, в яких вона виступає або другорядним об'єктом уваги і впливів, або предметом чергових соціальних експериментів і маніпуляцій. Безпека особистості повинна бути забезпечена політичними, економічними і правовими засобами і способами. На жаль, процес правового забезпечення взаємовідносин особистості з державою в Україні ще далеко не завершений, а в умовах збройного конфлікту, реформування й політичної модернізації це загрожує особистості багатьма проблемами.

Процес формування та закріплення людиною своїх прав бере свій початок від виникнення людини як індивіда та формування його цілісно-орієнтаційних настанов, що саме по собі зумовлює виникнення правовідносин між суб'єктами, тобто учасниками таких відносин. Історія людини – це постійна боротьба за свої права, починаючи від природних, якими людина наділена від народження, та закінчуючи правом на вільний доступ до мережі Інтернет та поширюваного в його просторах контенту. Саме боротьба людини за свої права часто призводила до епохальних змін в суспільно-політичному житті різних країн, наслідком чого ставало переосмислення місця і ролі людини у відносинах з державою. Саме в умовах глобалізації, нових досягнень, яких прагне людина, нескінченних пошуках нових відкриттів класифікація прав людини буде лише розширюватися, що призведе до необхідності створення нових механізмів їх реалізації та нормативно-правового закріплення [3, с. 45].

На нашу думку, під правами і свободами людини слід розуміти сукупність соціально-політичних, економічних, етичних та інших норм, що визначають фундаментальні основи демократичного й гуманітарного статусу окремої особистості, її взаємини з іншими людьми, суспільством і державою.

Змістовно права людини можна звести до низки основних груп [4 – 11]:

- фізичні (життєві) права – це можливості людини, необхідні для її фізичного існування, для задоволення її біологічних, матеріальних потреб (зокрема, право на життя, фізичну недоторканність, безпечне природне середовище, житло, соціальний захист);
- особистісні права – це закріплені у Конституції України невід'ємні вид та міра можливої поведінки людини та громадянина, що належать їм від народження, реалізація яких залежить від волі кожної людини, які гарантуються державою, та які є засобами здійснення будь-яких інших прав і свобод людини та громадянина, (зокрема, право на ім'я, честь та гідність, свободу думки і слова);

- культурні (гуманітарні) права – можливості збереження та розвитку етнонаціональної самобутності, доступу до знань та інших духовних здобутків людства, до їх засвоєння, використання та участі у подальшому примноженні (зокрема, право на освіту, користування надбаннями культури і мистецтва, наукову, технічну та художню творчість, авторські права);

- економічні права – це можливості людини реалізувати засоби до існування, беручи участь у виробництві, розподілі й наданні матеріальних чи інших благ;

- політичні права – можливості громадян брати активну участь у політичному житті держави і суспільства, висловлювати свою громадянську позицію щодо дій влади, а також це воля громадян, спрямована на розвиток демократії у державі.

Окрім наведеної класифікації, всі права людини можуть поділятися на певні види й за іншими критеріями, а саме:

- за значенням для їх носія – основні (необхідні для його існування та розвитку) і неосновні (які не є життєво необхідними);

- за способом здійснення – активні (свобода “для”, тобто для вчинення активних дій) і пасивні (свобода “від”, тобто від втручання, перешкоджання з боку інших суб’єктів);

- за суб’єктом складом здійснення – індивідуальні (здійснюються переважно одноособово, наприклад, право на свободу вираження переконань, на виховання своєї дитини) і колективні (можуть бути реалізовані лише спільними діями групи носіїв права, наприклад, право на утворення громадських об’єднань, проведення мітингів, демонстрацій);

- за історичною послідовністю виникнення і визнання – права першого покоління прав людини (“громадянські”, тобто здебільшого фізичні, особистісні й політичні), другого покоління прав людини (здебільшого економічні, соціальні та культурні), третього покоління прав людини (солідаристські, тобто здебільшого колективні права або права колективних суб’єктів) [12, с. 10-12], а також права четвертого покоління прав людини.

Права людини найтіснішим чином пов’язані з її безпекою. За сучасною класифікацією ООН [13] забезпечення прав людини в будь-якій країні має здійснюватися в наступних сферах її безпеки: економічної безпеки, продовольчої безпеки; безпеки здоров’я; екологічної безпеки; особистої безпеки; громадської безпеки; політичної безпеки.

Виходячи зі світового досвіду розвитку прав людини, можна виділити основні принципи їх забезпечення:

- права людини належать їй від народження (людина як людина має право), вони є невід’ємними й невідчужуваними;

- права людини засновані на принципі рівності, вони гарантовані кожному, хто перебуває під юрисдикцією держави;

- права людини є вищою цінністю, а їх повага, дотримання і захист – обов’язок держави;

- права людини є засобом контролю за владою, обмежником всевладдя й свавілля держави;

- забезпечення прав і свобод людини не допускає дискримінації за будь-якою ознакою;

- здійснення прав і свобод конкретної людини не повинно порушувати права і свободи інших людей;

- основні права і свободи повинні бути єдиними на всій території держави;
- цивільні, політичні, економічні, соціальні та культурні права і свободи рівноцінні за своєю значущістю, єдині (неподільні) і взаємопов'язані;
- колективні права невіддільні від прав особистості, вони не повинні суперечити індивідуальним правам людини;
- права людини регулюються законом, тобто фундаментальні права людини повинні дотримуватися у будь-якій ситуації. Вони можуть бути обмежені тільки законом і виключно для зазначених в Конституції країни і в найважливіших міжнародно-правових актах цілей.

Стосовно останнього принципу зазначимо, що згідно з Конституцією України в інтересах національної безпеки допускається обмеження таких конституційних прав і свобод людини і громадянина: право на особисте та сімейне життя (ст. 32); право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ст. 34); право на свободу об'єднання у політичні партії та громадські організації (ст. 36); право збиратися мирно, без зброї і проводити збори, мітинги, походи і демонстрації (ст. 36); право на страйк (ст. 44). Оскільки забезпечення національної безпеки включає також протидію злочинам проти її основ, з метою їх попередження можуть бути обмежені такі права, встановлені в Конституції України: право на свободу та особисту недоторканність (ст. 29); право на недоторканність житла (ст. 30); право на таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (ст. 31) [14]. Наведений перелік прав і свобод, які підлягають обмеженню, співмірний з міжнародними зобов'язаннями держави, визначеними у Загальній декларації прав людини 1948 р., Міжнародному пакті про громадянські і політичні права 1966 р., Міжнародному пакті про економічні, соціальні і культурні права 1966 р., Конвенції про захист прав людини і основоположних свобод 1950 р. Обов'язковою умовою обмеження конституційних прав і свобод людини і громадянина є те, що воно може відбуватися лише на підставі та у випадках, визначених у законі, і, як правило, за рішенням суду. У національному законодавстві закріплено процесуальний порядок здійснення такого обмеження. Органи державної влади, органи місцевого самоврядування, їх посадові та службові особи залежно від фактичних обставин уповноважені самостійно або через звернення до суду обирати способи забезпечення національної безпеки. Водночас, як справедливо зазначає Ю. Ірха, відсутність належного контролю за їхньою діяльністю та недосконалість процедури притягнення винних осіб до юридичної відповідальності можуть призвести до надмірного обмеження конституційних прав і свобод людини і громадянина та пов'язаних із цим тяжких наслідків [15, с. 83].

Сьогодні визнання і дійсне дотримання прав людини – найважливіший критерій національної безпеки, демократичності й гуманістичності будь-якої країни світу. При цьому захист прав людини в міжнародному масштабі (легітимний, схвалений світовою спільнотою) не вважається втручанням у внутрішні справи країни.

Як уже зазначалося, категорію “права людини” багато в чому визначають такі поняття, як “свобода особистості”, “людський розвиток”, “безпека особистості”. Широко поширеним поняттям, особливо в останні роки, стало поняття свободи особистості. Хоча цей термін активно використовується в публічних виступах політичними діячами різних орієнтацій, усталеного в науці визначення цього поняття поки що немає.

Відзначаючи різний сенс, що надається поняттю “свобода”, Ш.-Л. Монтеск’є у своїй праці “Про дух законів” писав: “Немає слова, яке отримало б стільки різноманітних значень і справляло б настільки різне враження на розуми, як слово “свобода”. Одні називають свободою легку можливість скидати того, кого наділили тиранічною владою; інші – право обирати того, кому вони повинні підкорятися; треті – право носити зброю і чинити насильство; четверті – вбачають її в привілеї перебувати під управлінням людини своєї національності або підкорятися своїм власним законам” [16, с. 288].

Карл Ясперс, розмірковуючи про визначення свободи, відзначав: “Свобода – не предмет. Вона не володіє реальним існуванням у світі, яке ми, спостерігаючи, могли б досліджувати. Свобода як предмет наукового пізнання не існує. Тому свободу не можна визначити твердо встановленим поняттям” [17, с. 170].

Як відомо, людина є істотою суспільною, соціальною, вона залежить від суспільства і формується навколишнім їй суспільним середовищем. З іншого боку, не менш очевидно, що людина – це природна істота. Як “людська природна істота”, особистість наділена свідомістю і волею, що визначають її здатність протистояти природі і впливати на неї. Звідси найважливіша характеристика людини – її відносна автономія як індивіда стосовно і природи й суспільства.

У зв’язку з цим можна й потрібно вести мову про два аспекти розуміння свободи людини: природної, що полягає у безконтрольній реалізації вроджених інстинктів і програм поведінки, і свободи соціальної, або громадянської, в рамках деяких свідомих обмежень у реалізації цих програм, якщо вони суперечать прийнятим в існуючому суспільстві нормам поведінки. Напрямки вдосконалення цих свобод протилежні: досконалість природної свободи полягає в її безмежності, досконалість громадянської свободи – в її свідомій обмеженості, виходячи з інтересів суспільства.

Поки людина не усвідомлювала себе вільною істотою, вона перебувала поза політикою, сприймала існуючу над нею владу як щось природне й необхідне, що має силу божественного або природного закону. Політика приходить у життя людей тільки разом з відчуттям особистої свободи, в її здобутті.

Сучасне розуміння прав людини світовою спільнотою сформульовано у Загальній декларації прав людини, прийнятій ООН у грудні 1948 року, а також у низці інших документів ООН, об’єднаних у Міжнародному біллі про права людини. Білль включає такі документи, як Загальна декларація прав людини (1948 р.), Міжнародний пакт про економічні, соціальні і культурні права (1966 р.), Міжнародний пакт про громадянські і політичні права (1966 р.) та ін. Найважливіше значення має також Європейська Конвенція про захист прав людини (1950 р.).

У 1990 році міжнародною організацією United Nations Development Programm – Програма розвитку ООН (ПРООН) – було введено у широкий вжиток поняття “людський розвиток” [18]. Згідно з концепцією ПРООН, розвиток людини – це процес розширення свободи вибору. При цьому підкреслюється, що кількість варіантів вибору може бути нескінченною. Однак на всіх рівнях розвитку три найбільш важливих варіанти зводяться до можливості вибрати довге і здорове життя, здобувати знання і мати доступ до ресурсів, необхідних для підтримання гідного рівня життя [13]. Сама Концепція базується на чотирьох основних принципах:

- продуктивність – можливість досягати бажаного ефекту своєї діяльності й підвищувати його, повноцінно брати участь у процесі формування доходу і працювати за грошову винагороду. Тому економічне зростання – одна зі складових моделей розвитку людського потенціалу;

- рівність як апріорі рівні можливості людей. Усі бар'єри, що перешкоджають цьому в економічному й політичному житті, необхідно ліквідувати;
- стійкість – доступ до можливостей не тільки нинішнім, а й майбутнім поколінням;
- розширення можливостей, що припускає, що розвиток здійснюється зусиллями людей, а не лише в інтересах людей. Вони повинні постійно розширювати свою участь у процесі прийняття рішень, а також в інших процесах, що визначають їхнє життя.

Концепція розвитку людини визначає людську безпеку як можливість вільно використовувати право вибору в умовах свободи, і при відсутності небезпеки, а також повну впевненість в тому, що ці можливості збережуться і в майбутньому.

Розглядаючи проблему прав і свобод людини, слід коротко зупинитись на розумінні її в Україні. Радянський період української історії наклав суттєвий відбиток як на розуміння безпеки в цілому, так і на розуміння прав і свобод зокрема. У сталінській і брежнєвській конституціях було видно чіткий пріоритет соціально-економічних (тобто, загальнодержавних) прав над тими, які прийнято вважати природними і невід'ємними (тобто, прав конкретної людини). Формально зафіксувавши низку політичних прав (свобода слова, друку, зборів і мітингів, вуличних походів і демонстрацій), Конституція 1936 року обмовила можливість їх використання “відповідністю інтересам трудящих”. Деякі з прав людини в цій Конституції взагалі були відсутні навіть формально (наприклад, свобода пересування, не кажучи вже про право приватної власності). Основний акцент був зроблений не на простір свободи людини, а на “опіку держави”. Ліберальні цінності (свобода, незалежність, індивідуалізм і універсалізм, ринкова економіка, свобода в рамках закону), ворожі радянській державі, не згадувались навіть на рівні декларації.

Конституція 1936 року передбачала право громадян на працю, тобто “право на одержання гарантованої роботи з оплатою їх праці у відповідності з її кількістю і якістю”, право на відпочинок, право на матеріальне забезпечення в старості і в разі хвороби і втрати працездатності, право на освіту. Конституція СРСР 1977 року доповнила перелік проголошених соціальних прав громадян, додавши до них такі, як право на охорону здоров'я, право на житло, право на користування досягненнями культури, а також гарантувавши свободу на наукову, технічну й художню творчість.

Конституція України 1996 року закріпила систему владних відносин, яка на той момент фактично склалася – напівпрезидентську унітарну республіку з парламентом, реально позбавленим контрольних повноважень, відносно слабкою судовою системою, а також урядом без суттєвих політичних функцій і тому постійно залежним від прямої президентської підтримки. Загалом, безвідповідальність держави перед суспільством у новій Конституції України зберігалася майже на рівні радянських часів. Конституційна система захисту прав людини фактично не працює.

Другий розділ Конституції України “Права, свободи та обов'язки людини і громадянина”, що нараховує майже третину з загальної кількості конституційних норм, містить велику кількість прямих запозичень з двох загальновідомих міжнародних пактів ООН про права людини 1966 р., але при цьому в суто юридичному сенсі не розрізняє норми Міжнародного пакту про громадянські та політичні права, які держава мусить виконувати за будь-яких обставин, і положення Міжнародного пакту про економічні, соціальні та культурні права, можливість реалізації яких пов'язується, як відомо, з реальним економічним станом тієї або іншої країни. Йдеться про те, що соціально-економічні права, як правило, вважаються нормами прямої дії лише за наявності спеціальних офіційних коментарів, якими визначаються конкретні параметри судового

захисту так званих “позитивних”, тобто існуючих за рахунок активності держави, прав і свобод [8; 9; 12; 19].

Слід також звернути увагу на те, що в Європейській Конвенції 1950 року [18] йдеться про “права людини та основоположні свободи”, а в Конституції України 1996 року – лише про “права і свободи людини”. Це означає, що конституційний захист таких суб’єктів прав, як юридичні особи, не забезпечений.

В умовах глобалізації у забезпеченні безпеки людини й обмеженні її прав відбувається низка змін [21 – 22]. Це різке збільшення залежності рівня життя людей від інтересів транснаціональних компаній; зниження значущості фактора територіальної обумовленості, яке означає, що зміни в житті людини дедалі частіше й сильніше залежать від процесів, що відбуваються далеко від місця її знаходження; зниження ролі національних кордонів, які втрачають своє значення не тільки для торгівлі, капіталів та інформації, а й для ідей, моральних норм, національної культури і цінностей; зростання темпів зміни ринків і технологій, що сприяє прискоренню ритму життя і підвищенню рівня нестабільності в суспільстві.

Таким чином, права людини у концентрованому вигляді виражають основні життєво важливі інтереси особистості в сучасному вигляді. Одним з основних прав і свобод людини є право на недоторканість її особистого (приватного) життя. У цій сфері між окремою людиною й суспільством (державою) існують певні протиріччя. З одного боку, з позицій забезпечення національної безпеки, суспільство й держава бажають володіти певним (причому, максимально можливим) обсягом інформації про людину. З іншого боку, людина як індивід і істота мисляча, має право на певну частину особистої інформації, яка доступна тільки їй. Іншими словами, держава з метою забезпечення своєї безпеки бажає знати про кожного свого громадянина якомога більше, людина ж намагається дати державі лише найнеобхідніший (визначений у нормативно-правових актах) мінімум інформації про себе, причому, тільки за її згодою. Що ж стосується порушень прав людини на недоторканність її приватного життя, то їх можна представити таким чином:

- насильницьке порушення усамітненості індивіда або втручання в його особисті справи (підслуховування й перехоплення телефонних переговорів, Інтернет-повідомлень, перлюстрація кореспонденції тощо);
- оприлюднення відомостей особистого характеру про людину, які, з точки зору цієї особи, несприятливо впливають на її суспільний імідж або завдають їй болю і душевних страждань (навіть у тих випадках, коли поширювані відомості відповідають дійсності);
- виставлення людини в неправдивому світлі в очах оточуючих без її згоди;
- використання імені або зображення людини в інтересах тієї особи, яка його використовує.

Категорія “приватне життя” в принципі не має юридичного змісту; правове регулювання лише встановлює межі його недоторканності (“приватності”) і, відповідно, межі допустимого втручання. Не випадково право на недоторканність приватного життя в деяких правових системах визначається як “право бути наданим самому собі”.

Сьогодні право на приватність привертає все більшу увагу суспільства. Воно включається в каталог прав людини і закріплюється багатьма конституціями демократичних країн. Ідея законодавчого забезпечення недоторканності приватного життя набуває нового, більш глибокого сенсу.

Проблема регулювання процесу збору персональних даних, збереження інформації та інші супутні питання, пов’язані з роботою з персональними даними в нашій країні (а

отже і з забезпеченням недоторканності особистого життя), зараз є відносно вирішеною й відомою широкому колу юристів. Очевидно, що законодавство не досконале і потребує поліпшення, проте основні положення регулюються Законом України “Про захист персональних даних” [23]. Так, відповідно до ст. 12 зазначеного Закону, збирання персональних даних є складовою процесу їх обробки, що передбачає дії з підбору чи впорядкування відомостей про фізичну особу. Суб’єкт персональних даних повідомляється про володільця персональних даних, склад та зміст зібраних персональних даних, свої права, визначені цим Законом, мету збору персональних даних та осіб, яким передаються його персональні дані:

- у момент збору персональних даних, якщо персональні дані збираються у суб’єкта персональних даних;
- в інших випадках протягом тридцяти робочих днів з дня збору персональних даних.

Крім вищенаведеного Закону, юридичні та фізичні особи мають можливість вирішувати питання, пов’язані з власною інформаційною безпекою, використовуючи положення Цивільного кодексу України, Закону України “Про інформацію” та інші законодавчі акти України.

Однак реальна ситуація багато в чому відрізняється від нормативної моделі. У ЗМІ часто з’являються повідомлення про несанкціоновані підслуховування та інші порушення недоторканності особистого життя приватних осіб. Більше того, вже неодноразово публічно висловлювалися пропозиції про створення загальнонаціонального реєстру населення – централізованої бази даних, де накопичувалася б майже вичерпна інформація про індивіда. Незважаючи на те, що це обґрунтовувалося тим, що так буде зручніше і для держави, і для самої людини, серед широких верств населення України ця ідея підтримки не отримала.

Будь-якій країні необхідні закони – чіткі й детально опрацьовані, які містять гарантії від несанкціонованого втручання в особисте життя з боку державних і приватних організацій, а у випадках, коли таке втручання є об’єктивно необхідним і санкціоноване законом – обов’язкові процедури, які виключили б свавілля у здійсненні ними своїх повноважень.

Право на недоторканність приватного життя не може не піддаватися певним обмеженням, і такі обмеження є об’єктивно необхідними, щоб забезпечити інтереси переважної більшості населення країни, які, за визначенням, висловлюють “публічний інтерес” по відношенню до незначної частини населення, що займається протиправною діяльністю. У першу чергу, це стосується асоціальних особистостей – злочинців, економічних злочинців, членів організованих злочинних і мафіозних груп, а також терористичних організацій.

У цілому, вторгнення в приватне життя окремої людини може здійснюватися в різних варіантах: з боку держави і її структур; з боку окремих соціальних, національних і т.п. груп; і, врешті-решт, з боку окремих осіб. Недоторканість особистості практично будь-якої людини найбільш вразлива в інформаційній сфері. У Доктрині інформаційної безпеки України вказується, що життєво важливими інтересами особи в інформаційній сфері є [24]:

- забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;
- забезпечення конституційних прав людини на захист приватного життя;
- захищеність від руйнівних інформаційно-психологічних впливів.

Крім того, до засобів забезпечення недоторканності приватного життя відносяться Закони України “Про інформацію” [25] і “Про державну таємницю” [26]. Однак питання про те, яка ж інформація повинна вважатися відкритою, а яка закритою, і якою повинна бути відповідальність за розголошення службової чи комерційної інформації, як і раніше остаточно не вирішені, оскільки відсутня відповідна необхідна законодавча база.

Можна стверджувати, що небезпечними для дотримання прав і свобод людини слід вважати такі інформаційні впливи, які загрожують дестабілізуючими, деструктивними, такими, що ущемляють інтереси особистості, суспільства й держави результатами. Оскільки повна відсутність загроз (у тому числі в інформаційній сфері) – недосяжний ідеал для нашого небезпечного світу, то безпека людини визначається можливостями попереджати, відбивати, нейтралізовувати небезпечні інформаційні впливи.

Проблема забезпечення безпеки і проблема дотримання прав і свобод людини досить часто виявляються в певному протиріччі одна з одною. Так, наприклад, Д. Смайлі вказує на те, що “окремі ліберали, прогресивні і демократи визнають, принаймні інтуїтивно, що “національна безпека” є кодовим словом для трайбалізму, в той час як “права людини” є кодовим словом для верховенства права” [27]. Витоки цього протиріччя лежать у суперечності між нахилами, правами й інтересами окремих індивідів і їх об’єднань, з одного боку, та інтересами великих людських спільнот, частиною яких вони є, з іншого. У більш широкому плані – це протиріччя між інтересами меншості й більшості. І оскільки забезпечення безпеки, як правило, пов’язано передусім з інтересами більшості членів суспільства, обмеження прав і свобод меншини, інтереси та діяльність якої (або багатьох представників якої) часом представляють реальну або потенційну небезпеку для суспільства, є виправданим [28 – 30].

Загрози безпеці так чи інакше виникають внаслідок кримінальної або іншої загрозової для національних інтересів діяльності, яка здійснюється різними організаціями, соціальними групами, корпоративними об’єднаннями та іншими колективами, організованими для задоволення певних інтересів, спрямованих (повністю або частково) проти інтересів особистості, суспільства і держави. Тому люди, що входять у такі об’єднання, виявляються під підозрою, хоча вина їх далеко не завжди очевидна, а в багатьох випадках вони не беруть участь і не несуть ніякої відповідальності за антидержавну і антигромадську діяльність спільнот, до яких належать. У зв’язку з цим у всіх демократичних країнах вирішення завдань профілактики й нівелювання загроз національній безпеці в різних сферах, так само як і безпеці взагалі, здійснюється з урахуванням того, наскільки вжиті заходи адекватні існуючим загрозам і поєднуються з конституційними вимогами забезпечення прав і свобод людини і громадянина. Постійна постановка і обговорення цього питання у багатьох країнах, у тому числі і в Україні, особливо активно ініціюється правозахисними організаціями. Це обумовлене тим, що безпека (а мова при цьому йде частіше за все не про безпеку окремо взятої людини, а про безпеку суспільства) не може бути в багатьох випадках забезпечена без певного обмеження прав і свобод окремих індивідів і навіть соціально-етнічних груп (у тому числі і їх права на вільне пересування і вибір місця проживання).

Тут слід зауважити, що узагальнені принципи обмеження прав людини встановлені міжнародними нормами. Зокрема, ст. 29 Загальної декларації прав людини проголошує, що при здійсненні своїх прав і свобод кожною людиною до неї застосовуються тільки такі обмеження, які встановлені законом винятково з метою забезпечення гідного визнання та поваги до прав і свобод інших і задоволення справедливих вимог моралі суспільного порядку та загального благополуччя в демократичному суспільстві [31].

Відповідно до ст. 10 Європейської Конвенції з прав людини, яка встановлює обмеження щодо права на вираження своєї думки, такі обмеження мають бути [20]: 1) встановлені законом; 2) бути необхідними в демократичному суспільстві; здійснюватися в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров'я чи моралі, для захисту репутації чи прав інших людей, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету та безсторонності суду. Подібні обмеження встановлені щодо окремих прав і свобод. При цьому, наприклад, під "необхідністю в демократичному суспільстві" Європейський Суд з прав людини (рішення ЄСПЛ від 24.03.1988 р., параграф 67) тлумачить, що будь-яке втручання (обмеження) в реалізацію права повинно відповідати "нагальній суспільній потребі" [32]. Слід зазначити, що наведені міжнародно-правові вимоги з незначними відмінностями втілені у ч. 3 ст. 34 Конституції України, яка встановлює право кожного на свободу думки і слова, на вільне вираження своїх поглядів і переконань та право на інформацію. Названі конституційні положення через відсутність узагальнюючої норми формально можна екстраполювати на визначення законної мети обмеження інших конституційних прав і свобод [33, с. 129].

Стосовно окремо взятої людини, забезпечення її особистої й колективної безпеки в соціумі (зрозуміло, разом з самим цим соціумом, невід'ємною складовою якого вона є) вже саме по собі повинно розглядатися як одне з найважливіших прав людини. І хоча це в явному вигляді не записано в міжнародних актах про права людини, аналіз цих актів, зокрема таких основоположних, як Загальна декларація прав людини [30], Міжнародний пакт про економічні, соціальні і культурні права [34] і Міжнародний пакт про громадянські і політичні права [35], свідчить про те, що це саме так. У цих актах в числі прав і свобод людини називаються, зокрема, і такі, як право на життя, свободу та особисту недоторканність; право на вільний розвиток її особистісних прав в економічній, соціальній і культурній галузях; право на справедливі й сприятливі умови праці; право на достатній життєвий рівень для неї самої і її сім'ї, що включає достатнє харчування, одяг і житло, неухильне поліпшення умов життя; право на найвищий досяжний рівень фізичного і психічного здоров'я тощо.

Зіставлення цих та багатьох інших прав, зафіксованих у вказаних та інших міжнародних актах про права людини, з напрямками забезпечення національної безпеки в різних сферах діяльності, показує, що основною метою і напрямками забезпечення безпеки якраз і є створення мінімально необхідних (тобто, у першу чергу безпечних) умов для реалізації зазначених прав.

Існування зазначеного протиріччя між необхідністю забезпечення безпеки як переважно колективного права і індивідуальними правами і свободами людини, протиріччя між необхідністю забезпечення прав більшості і меншості, окремих індивідів і іншою частиною соціуму по суті визнається і в зазначених міжнародних актах. Для можливості хоча б часткового вирішення цієї суперечності у Загальну декларацію прав людини включено положення про те, що "при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших і дотримання справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві" (ст. 29) [31]. З метою розвитку цього положення Міжнародний пакт про громадянські і політичні права встановив як підстави для застосування зазначених обмежень "охорону державної безпеки, громадського порядку, здоров'я, моральності населення або прав і свобод інших" (ст. 12) [35].

Значна частина цих правил відображається з різними варіаціями в конституціях більшості демократичних держав, у тому числі і в Конституцію України.

Політики і політологи, які трактують демократію як підпорядкування меншості більшості, вважають, що забезпечення безпеки пов'язане, у першу чергу, з інтересами більшості членів суспільства. Тому, як зазначалося вище, обмеження прав і свобод меншості, інтереси, цінності і цілі якої можуть представляти реальну або потенційну небезпеку для суспільства – виправдано. Прихильники новітніх концепцій демократії, які вважають її визначальним критерієм захисту прав меншин і конкретних людей, вважають, що подібні міркування покликані виправдовувати недемократичну політику урядів, які допускають кричущі порушення прав і свобод людини під приводом забезпечення національної безпеки [36].

У зв'язку з цим, різкій критиці з боку міжнародних правозахисних організацій піддаються ті демократичні країни, які спочатку опікувалися правами людини, а після 11 вересня 2001 року різко змінили орієнтацію і вдалися до надзвичайних заходів у боротьбі з тероризмом.

Висновки.

Права людини і національна безпека тісно взаємопов'язані і доповнюють одне одного. У демократичних країнах національна безпека означає, перш за все, засіб забезпечення громадянського миру і особистих прав громадян. І те, і інше є необхідним для довгострокової стабільності і благополуччя країни. Вільні й демократичні держави, які дотримуються прав своїх громадян, допомагають закласти основу і для міжнародного миру. Навпаки, держави, які грубо й систематично порушують права людини, найчастіше починають створювати загрози для сусідніх країн і міжнародної спільноти.

В Україні, як і в більшості держав світу, категорія “національна безпека” охоплює значне коло питань у різних сферах суспільного життя. Цілком погодимося з точкою зору Ю. Ірхи, що це дозволяє надто широко тлумачити її зміст і, як наслідок, довільно оперувати ним при обмеженні прав і свобод людини і громадянина та при покаранні осіб, які своїми висловлюваннями чи діями їй загрожують. Крім того, сфера забезпечення національної безпеки є надзвичайно складною для реформування та контролю, оскільки з об'єктивних причин відомостями про реальне становище у державі та суспільстві володіє досить обмежена кількість людей [15, с. 81].

Реальна взаємозумовленість феноменів національної безпеки і прав людини часто носить суперечливий характер. Часто витоки вказаного протиріччя лежать у поділі між інтересами, цінностями й цілями окремих індивідів і їх об'єднань, з одного боку, і інтересами великих людських спільнот, частиною яких вони є, з іншого.

Прихильники новітніх концепцій демократії [37 – 39], які вважають її визначальним критерієм захисту прав меншин і конкретних людей, вважають, що міркування про припустимість обмеження прав людини для забезпечення національної безпеки покликані виправдовувати недемократичну політику урядів, які допускають порушення прав і свобод людини під приводом забезпечення національної безпеки. У зв'язку з цим, міжнародні правозахисні організації пропонують законопроекти, суттю яких є теза про те, що безпека і права людини – не альтернатива. Одне від іншого невіддільне. Повага до прав людини і є шлях до безпеки, а не перешкода на цьому шляху.

Права і свободи особистості виступають сьогодні як один із найважливіших об'єктів політики національної безпеки. Фіксуючи реальну захищеність і гарантуючи права і свободи особистості в конкретній спільноті, права людини можуть виступати як

гуманістичний орієнтир розвитку не тільки держави в цілому, але й системи національної безпеки, яка склалася в країні. При цьому проблема взаємозалежності національної безпеки і прав людини не є проблемою вибору за принципом “або/або”. Це – проблема компромісу між забезпеченням національної безпеки і дотриманням прав людини, між реалізацією прав людини і захистом національної безпеки.

Використана література

1. Крутов В.В. Концептуально-правові основи забезпечення національної безпеки крізь призму духовності людини. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 191-201.
2. Burke-White W.W. Human Rights and National Security: The Strategic Correlation. *Harvard Human Rights Journal*. 2004. Vol. 17. P. 254. URL: <https://www.law.upenn.edu/cf/faculty/wburkewh/workingpapers/.pdf> (дата звернення: 12.12.2019).
3. Марченко М.А. Формування та розвиток ідеї прав людини в історико-правовій думці. *Бюлетень Міністерства юстиції України*. 2019. № 2. С. 42-46.
4. Пейн Т. Права людини. Львів: Літопис, 2000. 287 с.
5. Перлін Дж. Права людини: концепції, підходи, реалізація. Київ: Ай-Бі, 2003. 262 с.
6. Філософія прав людини / за заг. ред. Ш. Госепата та Г. Ломанна. Київ: Ніка-Центр, 2008. 320 с.
7. Чепульченко Т.О. Права людини як мета та межі правотворчості. *Альманах права*. 2019. Вип. 10. С. 348-353.
8. Білозьоров Є.В. Права людини в умовах глобалізації: доктринальний підхід. *Науковий часопис НПУ імені М.П. Драгоманова. Серія 18: Економіка і право*. 2012. Вип. 18. С. 79-84.
9. Хальота А.І. Конституційні особисті права та свободи людини і громадянина та їх забезпечення органами внутрішніх справ: автореф. дис. ...канд. юрид. наук. Київ, 2004. 19 с.
10. Пустовіт Ж.М. Актуальні проблеми прав і свобод людини і громадянина в Україні: навчальний посібник. Київ: КНТ, 2009. 232 с.
11. Букач В.В. Конституційні політичні права та їх забезпечення міліцією: автореф. дис. ...канд. юрид. наук. Київ, 2004. 20 с.
12. Рабінович П.М., Хавронюк М.І. Права людини і громадянина: навчальний посібник. Київ: Атіка, 2004. 464 с.
13. Доклад о человеческом развитии – 2019. URL: http://hdr.undp.org/sites/default/files/hdr_2019_overview_-_russian.pdf (дата звернення: 15.05.2020).
14. Конституція України: Закон України від 28.06.96 р. № 254/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80/> (дата звернення: 26.05.2020).
15. Ірха Ю. Обмеження конституційних прав і свобод людини і громадянина в інтересах національної безпеки України в сучасних умовах. *Вісник Конституційного суду України*. 2015. № 5. С. 78-87.
16. Монтескьє Ш.-Л. Избранные произведения / общ. ред. и вступ. статья проф. М.П. Баскина; примеч. Р.С. Миндливоной. Москва: Госполитиздат, 1955. 800 с.
17. Ясперс К. Смысл и назначение истории / пер. с нем.; вступ. ст. П.П. Гайденко. Москва: Политиздат, 1991. 527 с.
18. Программа развития Организации Объединенных Наций. URL: <https://www.un.org/ru/sections/general/documents/> (дата звернення: 14.05.2020).
19. Захаров Є. Конституція і права людини. URL: <http://khpg.org/index.php?id=1561894103> (дата звернення: 15.05.2020).
20. Європейська Конвенція з прав людини. URL: https://www.echr.coe.int/Documents/Convention_UKR.pdf (дата звернення: 15.05.2020).
21. Білас І.Г. Сучасні виклики і загрози правам людини в умовах глобалізації. *Актуальні проблеми міжнародних відносин*. 2013. Вип. 117 (1). С. 17-25.

22. Білозьоров Є.В. Права людини в умовах глобалізації: доктринальний підхід. *Науковий часопис НПУ імені М.П. Драгоманова. Сер. 18: Економіка і право*. 2012. Вип. 18. С. 79-84.
23. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 15.05.2020).
24. Доктрина інформаційної безпеки України. URL: <https://zakon.rada.gov.ua/laws/show/47/2017> (дата звернення: 15.05.2020).
25. Про інформацію: Закон України від 02.10.92 р. № 2658-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 15.05.2020).
26. Про державну таємницю: Закон України від 21.01.94 р. № 3856-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12> (дата звернення: 15.05.2020).
27. Smiley J. Why human rights are more important than national security. URL: http://www.huffingtonpost.com/jane-smiley/why-human-rightsare-more_b_73286.html (дата звернення: 26.05.2020).
28. Бражник В.О., Сидоренко Д.А. До питання обмеження прав і свобод людини в умовах дії спеціального правового режиму. *Міжнародний науковий журнал "Інтернаука"*. 2018. № 9(3). С. 10-14.
29. Дахова І.І. Обмеження реалізації прав і свобод людини: конституційне регулювання та практика Європейського Суду з прав людини. *Форум права*. 2018. № 4. С. 17-25.
30. Андрієвська О.В. Формальні підстави обмеження прав і свобод людини і громадянина в Україні. *Право і суспільство*. 2016. № 1. С. 3-8.
31. Всеобщая декларация прав человека. URL: http://www.consultant.ru/document/cons_doc_LAW_120805/ (дата звернення: 12.05.2020).
32. Олссон (Olsson) против Швеции. Судебное решение от 24 марта 1988 г. URL: <http://www.echr.ru/documents/doc/2461423/2461423.htm> (дата звернення: 23.05.2020).
33. Костецька Т.А., Андрієвська О.В. Щодо поняття конституційно-правових обмежень прав і свобод людини і громадянина: теоретичні аспекти. *Правова держава*. 2018. Вип. 29. С. 122-131.
34. Международный пакт об экономических, социальных и культурных правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactecon.shtml (дата звернення: 12.05.2020).
35. Международный пакт о гражданских и политических правах. URL: https://www.un.org/ru/documents/decl_conv/conventions/pactpol.shtml (дата звернення: 12.05.2020).
36. Защита прав человека в условиях глобальной войны с терроризмом. URL: <http://www.mhg.ru/editions/chronic/> (дата звернення: 10.01.2020).
37. Андрійчук Т.С. Сучасні концепції демократії у працях французьких дослідників. *Вісник Національного технічного університету України "Київський політехнічний інститут". Політологія. Соціологія. Право*. 2012. № 1. С. 12-17.
38. Колодій А.Ф. Концепція публічного (нового) врядування в її застосуванні до демократичних і перехідних систем. *Демократичне врядування*. 2012. Вип. 10. URL: http://nbuv.gov.ua/UJRN/DeVr_2012_10_3 (дата звернення: 16.05.2020).
39. Иванцова Н.І., Москальова Н.П. Концепція плюралістичної демократії: від плюралізму до неокорпоративізму. *Сучасне суспільство*. 2014. Вип. 2. С. 67-77.

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

УДК 342.727

**КОСІЛОВА О.І.**, кандидат політичних наук, доцент, юридичний факультет  
Київського національного університету ім. Тараса Шевченка.  
ORCID: <https://orcid.org/0000-0002-5574-3771>.

## ТЛУМАЧЕННЯ СТАТТІ 21 КОНСТИТУЦІЇ УКРАЇНИ У КОНТЕКСТІ ЄВРОПЕЙСЬКОЇ ПРАВОВОЇ ДОКТРИНИ

**Анотація.** У статті аналізуються основоположні природні права людини – право на свободу, на рівність, на людську гідність, а також принципи невідчужуваності та непорушності прав, закріплені у статті 21 Конституції України. Права та принципи прав людини аналізуються з позицій європейських стандартів прав людини, зокрема німецької правової доктрини.

**Ключові слова:** право на свободу, право на людську гідність, право на рівність, принцип рівності, принцип невідчужуваності, принцип непорушності прав, рішення Конституційного Суду України, рішення Федерального Конституційного Суду.

**Summary.** The article analyzes fundamental natural human rights, such as the right to liberty, to equality, to human dignity, as well as principles inalienability of inviolability of rights enshrined in Article 21 of the Constitution of Ukraine. Human rights and principles are analyzed from the standpoint of European human rights standards, in particular German legal doctrine.

**Keywords.** The right to liberty, the right to human dignity, the right to equality, the principle of equality, the principle of inalienability, the principle of inviolability of rights, decisions of the Constitutional Court of Ukraine, decisions of the Federal Constitutional Court.

**Аннотация.** В статье анализируются основополагающие естественные права человека – права на свободу, на равенство, на человеческое достоинство, а также принципы неотчуждаемости и незаблемости прав, закрепленные в статье 21 Конституции Украины. Права и принципы прав человека анализируются с позиций европейских стандартов прав человека, в частности немецкой правовой доктрины.

**Ключевые слова.** Право на свободу, право на человеческое достоинство, право на равенство, принцип равенства, принцип неотчуждаемости, принцип незаблемости прав, решение Конституционного Суда Украины, решение Федерального Конституционного Суда.

**Постановка проблеми.** Права людини в сучасному світі утворюють складний комплекс, що існує як на рівні національного законодавства, так і на рівні міжнародного права. Права на свободу та людську гідність є основоположними природними правами, що надаються кожній особі від народження. Водночас, окремими свободами володіють лише громадяни конкретної держави. Принцип рівності, який формально проголошує загальну рівність людей у здійсненні прав та свобод, насправді також значною мірою залежить від факту наявності (або відсутності) громадянства та інших чинників. Загальний перелік прав і свобод приблизно однаковий у більшості конституцій сучасних демократичних держав, але кожна країна має свої особливості нормативного їх закріплення, як і механізм їх реалізації.

**Результати аналізу наукових публікацій.** Права і свободи людини є предметом наукового аналізу багатьох вчених правознавців, філософів, соціологів. Серед представників юридичної науки дослідження прав і свобод людини і громадянина здійснювали О. Гришук, П. Рабінович, Р. Мельник, Т. Чехович, І. Полховська, З. Ромовська, О. Васильченко, Б. Банашак, С. Вдовіченко, І. Головань, М. Гультай,

В. Кампо, В. Овчаренко, М. Савчин, Є. Шишкіна, Т. Фулей, Н. Шукліна, М. Антонович, О. Совгіря, С. Головатий, В. Бесчастний, О. Філонов, В. Субботін, С. Пашков, О. Петришин та інші дослідники. Серед сучасних німецьких дослідників у цій сфері варто відзначити Г. Яраса, Г. Гезер, Б. Вілса, Ж. Шустера, П. Хюбера, М. Кюніха, Г. Еллінека та інших.

У статті 21 Конституції України закріплено основоположні права на свободу, на людську гідність, а також принципи рівності, невідчужуваності та непорушності прав, що деталізуються у її наступних статтях. Таким чином, її можна вважати базовою для всіх інших прав людини і громадянина.

У вітчизняній правовій науці права на свободу та гідність досліджуються, здебільшого окремо, без їх взаємозв'язку з іншими правами. У зв'язку з цим вважаємо за доречне дослідити права та принципи, закріплені у статті 21 Конституції України у відповідності до європейської правової доктрини, зокрема досвіду Федеративної республіки Німеччини.

**Метою статті** є визначення сутності та змісту основоположних прав на свободу, на рівність, на людську гідність, а також принципи невідчужуваності та непорушності прав, що закріплені у статті 21 Конституції України відповідно до міжнародних стандартів прав людини. Для реалізації поставленої мети слід з'ясувати правову природу гідності людини; визначити зміст правових категорій “свобода”, “рівність”, “гідність”; дослідити зміст принципів невідчужуваності та непорушності прав.

**Виклад основного матеріалу.** Конституція України встановлює, що всі люди є вільні і рівні у своїй гідності та правах, що права і свободи людини є невідчужуваними та непорушними (ст. 21) [1]. Для здійснення тлумачення цієї статті перш за все слід розмежувати поняття “людина” та “громадянин”.

На думку українських науковців В.М. Бесчастного, О.В. Філонова, В.М. Субботіна, С.М. Пашкова “людина”, як родове поняття, вживається для характеристики певних біологічних рис *homo sapiens*, що виокремився на певній стадії розвитку з біологічного середовища. Під “людиною” у цьому випадку також розуміється, що це єдина жива істота, наділена свідомістю. Тоді як “громадянин” позначає фізичну особу, чий правовий статус обумовлений належністю до тієї або іншої держави. Громадяни в кожній країні становлять найчисленнішу категорію населення. Саме вони наділені правами і свободами в найбільш широкому обсязі. Однак якщо права людини впливають із самої її природи і не можуть бути обумовлені будь-чим, то права громадянина визначаються фактом громадянства [2, с. 70-71].

Важливо, що основоположні права є невід'ємними, постійними і закріпленими. Кожен може поспиратися на захист своїх прав проти держави. Ці права закріплено у тексті Основного Закону як права “кожного”, “будь-кого”, “нікого” або “всіх людей”. Отже, у ст. 21 Конституції України наголошується на всезагальному характері прав і свобод людини як родового поняття, як живої істоти, що наділена розумом. До уваги не беруться інші види конституційно-правового статусу та особистісні риси. Тобто, основні права і свободи закріплюються за кожною людиною, незалежно від факту наявності чи відсутності у неї громадянства певної держави.

У широкому розумінні під свободою можна розуміти можливість людини приймати рішення за власним бажанням [3]. Свобода приймати рішення, означає вибір між різними можливостями; свобода означає не тільки самовизначення, але і завжди відповідальність за прийняті рішення.

Характерною рисою німецької правової доктрини є тлумачення свобод крізь призму прав людини. Термін “свобода” не є чітко визначеним в Основному законі ФРН.



Скоріше Конституція у формі основних прав стала букетом багатьох свобод. Права – це свобода. Основні права розглядаються як способи (виміри) вільного розвитку особистості (у розумінні ст. 2 п. 1 Конституції) [4].

Свобода (вільність) як фундаментальна якісна характеристика людини відображає свободу її волі, тобто здатність свідомо, самостійно й добровільно обирати той чи інший варіант поведінки, діяльності як інтелектуальної, розумової, так і фізичної [5]. Звернемось до сучасного розуміння свободи – свобода є фундаментальною характеристикою людського існування, універсальною характеристикою людського буття; свобода стосується здатності людини обирати своє буття та керувати ним [6]. З юридичної точки зору свобода – це суб'єктивна можливість людини і громадянина здійснювати або не здійснювати певні дії, засновані на його конституційних правах та свободах [7]. З філософської точки зору існують такі види свобод людини: свобода волі людини – свідомо свобода вибору у житті, приватних життєвих рішеннях, обранні життєвих пріоритетів, організації свого життя тощо; суспільна свобода громадянина – права людини в суспільстві та державі, регульована законами; духовна свобода особистості – християнське розуміння свободи духу від рабства гріху та гріховних пристрастей (тобто від своїх же пристрастей та злих звичок, напр. від гніву, нетерпеливості, осуду, жадібності, заздрості, надмірних пожадань плоті тощо) [6].

Конституційний Суд України визначає право на свободу як невід'ємне та невідчужуване конституційне право людини, яке передбачає можливість вибору своєї поведінки з метою вільного та всебічного розвитку, самостійно діяти відповідно до власних рішень і задумів, визначати пріоритети, робити все, що не заборонено законом, безперешкодно і на власний розсуд пересуватися по території держави, обирати місце проживання тощо. Право на свободу означає, що особа є вільною у своїй діяльності від втручання, за винятком обмежень, які встановлюються Конституцією та законами України [8].

М. Савчин вважає, що вказане рішення Конституційного Суду України стосується визначення меж для встановлення законодавцем підстав для обмеження свободи індивіда. Суд послався на положення ст. 5 Конвенції про захист прав людини і основоположних свобод та відповідне прецедентне право Європейського Суду з прав людини, якими власне Верховна Рада Україна зв'язана згідно засад поваги до міжнародних стандартів захисту прав людини, мінімальних вимог захисту яких держава має додержуватися у своєму національному законодавстві [9, с. 115].

Концепція свободи, закріплена у Конституції ФРН, вимагає обмеження законами основних прав. Свобода основних прав сама по собі є двозначною: в основному права особи діяти на власний розсуд обмежуються державним органом, який визначає межі дозволених дій. Свобода людини є недоторканною, а втручання у свободи людини можливо лише на підставі закону (ст. 2, п. 2). Таким чином, приватна автономія обмежена суспільною автономією [10, с. 237; 11, с. 109]. Німецький правознавець Ханс Х. Рапп, аналізуючи класичні громадянські права, підкреслює, що це права на свободу, які захищають сфери особистої відповідальності, поведінки або індивідуальної діяльності [12, с. 577]. Вони мають на меті оборону і спрямовані проти будь-якого втручання держави, яке не відповідає критерію суворої обґрунтованості потребами загального блага.

На нашу думку, свобода є фундаментальною цінністю для людини, але вона повинна мати свої кордони, межі, щоб не стати свавіллям, насильством над іншими людьми, тобто не перетворитися на неволю. Межі народного суверенітету закінчуються там, де починається “незалежність приватної особи і особисте життя”. Наявність цих

меж перетворює стримування влади і контроль над нею на основний принцип політико-інституційного устрою суспільства [13, с. 42].

Важливим елементом ст. 21 Конституції України є прив'язка до гідності людини, оскільки “всі люди є вільні та рівні у своїй гідності і правах” [1]. Загалом гідність можна визначити як об'єктивну властивість людини, яка відображає її унікальну, неперевершену цінність. У науково-практичному коментарі до Конституції України наголошено на тому, що людську гідність слід трактувати як право, гарантоване ст. 28 Конституції України, і як конституційну цінність, яка наповнює сенсом людське буття, є фундаментом для усіх інших конституційних прав, мірилом визначення їх сутності та критерієм допустимості можливих обмежень таких прав [5].

Право на людську гідність тлумачиться сучасними вітчизняними та зарубіжними дослідниками як визначальне природне право особи. У випадках порушення якогось права людини чи якоїсь свободи завжди принижується її гідність. В Україні право на людську гідність розцінюється як рівнозначне та співмірне з іншими правами, такими як право на життя, на свободу тощо. Тоді як в інших державах, зокрема у Німеччині право на людську гідність є найвищою конституційною цінністю та джерелом всіх інших прав людини.

На нашу думку, гідність людини слід розуміти як ідею про те, що всі люди мають однакову цінність незалежно від будь-яких особливостей (рис), таких як походження, стать чи вік. З юридичної точки зору право на людську гідність належить до природних прав людини і становить одну з головних правових цінностей, яка слугує критерієм оцінки конституційності та законності актів, дій/бездіяльності державних органів і посадових осіб, фізичних та юридичних осіб.

З моменту народження людини її гідність є однаковою, “рівною” із гідністю інших. Усвідомлення цього усіма приводить до формування у кожної особи почуття власної гідності, очікування поваги до неї з боку інших людей, установку на відстоювання своїх прав, а також визнання нею рівних прав усіх інших людей. Однаковість гідності кожної людини відображено й у тій нормі Конституції, за якою “кожен має право на повагу до його гідності” [5].

Слід також відзначити, що чинне законодавство України хоча і приділяє значну увагу людській гідності та правам і свободам людини, не містить визначення понять гідності, як і суміжних категорій, таких як честь, ділова репутація тощо. Це пояснюється тим, що вони є морально-етичними категоріями й одночасно особистими немайновими правами, яким закон надає значення самостійних об'єктів судового захисту, тому їх зміст, обсяг, сферу захисту доволі складно визначити.

У Конституції України людська гідність має особливе значення та нормативне закріплення. Зокрема, “людина, її життя і здоров'я, честь і гідність визнаються в Україні найвищою соціальною цінністю” (ч. 1 ст. 3); “усі люди є вільні і рівні у своїй гідності та правах” (ст. 21); “кожен зобов'язаний неухильно додержуватися Конституції України та законів України, не посягати на права і свободи, честь і гідність інших людей” (ч. 1 ст. 68). Вказані положення Основного Закону України корелюють із міжнародними та європейськими стандартами щодо “гідного людського життя”, “мінімальних вимог існування в умовах, гідних людини”, прав людини “не зазнавати голоду” та на “захист від бідності”, якими має керуватися соціальна держава [14].

Гідність людини – це її цінність як такої, самої по собі, яка не залежить від будь-яких індивідуальних властивостей (біологічних чи соціальних). Як зазначає О.В. Петришин, засада рівності всіх людей впливає з огляду саме на їх “антропну” гідність: “Антропна гідність людини – це її самоцінність як родової біосоціальної істоти, змістовно зумовлена

насамперед існуючими суспільними відносинами, а також іншими факторами людського буття. Психічним (ідеальним) відображенням цієї органічної, “природженої” властивості кожної людини є її власні, а також інших суб’єктів суспільства оціночні судження стосовно зазначеної властивості, тобто оцінки гідності людини” [5].

Відповідно до німецької правової доктрини, людська гідність є причиною існування всіх прав людини. В ст. 1 Основного Закону ФРН зазначено: “Гідність людини непорушна. Поважати і захищати її є обов’язок всіх державних органів”. Цим твердженням починається преамбула не тільки розділу основоположних прав, але ним пронизано і весь текст Основного Закону [4].

Показовим рішенням Федерального конституційного суду Німеччини щодо захисту права на людську гідність є рішення 2006 року стосовно Закону “Про авіаційну безпеку” (LuftSiG), який був прийнятий у відповідь на теракти 11 вересня 2001 року. У ньому Суд зазначає, що людське життя є життєво важливою основою гідності людини як основного конституційного принципу та вищої конституційної цінності. Відповідно до нього, кожна особа володіє людською гідністю, незалежно від її особистих якостей, фізичного чи психічного стану, досягнень та соціального статусу. Гідність не можна відняти у людини. Це твердження стосується кожного, незалежно від ймовірної тривалості життя людини [15].

У своєму рішенні Суд наголосив, що “...даючи вказівку на знищення літака, який захопили терористи держава розпоряджається життям пасажирів в односторонньому порядку, тим самим позбавляє їх самоцінності. Відповідно до дії ст. 1 (1) Основного Закону (гарантія людської гідності), закон є нікчемним, якщо на його підставі передбачається вбивство невинних людей, які опинилися в безпорадній ситуації” [15].

Щодо конституційного принципу рівності, то його деталізований склад закріплений у ст. 24 Конституції та має такі аспекти прояву: 1) рівність прав і свобод (рівноправність) незалежно від будь-яких ознак: раси, кольору шкіри, політичних, релігійних та інших переконань, статі, етнічного та соціального походження, майнового стану, місця проживання, за мовними або іншими ознаками; 2) рівність перед законом; 3) рівноправність жінки і чоловіка (гендерна рівність).

Конституційний Суд України зазначає, що “гарантована Конституцією України рівність усіх людей в їх правах і свободах означає необхідність забезпечення їм рівних правових можливостей як матеріального, так і процесуального характеру для реалізації однакових за змістом та обсягом прав і свобод” [16].

Держава гарантує рівні можливості у виборі професії та роду трудової діяльності (ч. 2 ст. 43); діти рівні у своїх правах незалежно від походження (ч. 1 ст. 52); усі учасники судового процесу рівні перед законом і судом (ч. 3 п. 2 ст. 129) [1]. Конституція України передбачає рівне право всіх громадян на свободу об’єднання в політичні партії та громадські рухи (ст. 36), рівне право доступу до державної служби, служби в органах місцевого самоврядування (ст. 38). Немає ніяких обмежень у тому числі за ознакою статі, у праві на власність (ст. 41), підприємницьку діяльність (ст. 42), працю (ст. 43), соціальний захист (ст. 46), інші політичні та соціально-економічні права тощо [1].

Як зазначає К. Чижмарь, розвиток усіх форм власності поряд із визнанням приватної власності є необхідною умовою та передумовою для набуття кожною людиною (рівною мірою жінкою і чоловіком) економічної свободи, без якої немає і не може бути свободи політичної [17].

Приклади прав рівності, закріпленими в тексті Основного Закону ФРН також є: право на рівність всіх людей, право на рівність чоловіків і жінок, право на рівне ставлення не залежно від статі, походження, раси, мови, країни походження, релігійні чи

політичні погляди (ст. 3 п. 1-3), право позашлюбних дітей користуватися однаковими умовами для їх фізичного та психічного розвитку, як і дітей, що народилися у шлюбі (ст. 6 п. 5), право на однакові громадянські права та обов'язки у кожній федеральній землі для кожного німця; право кожного німця на рівний доступ до будь-якої державної посади [4].

Таким чином, у цілому положення Конституції України відповідають міжнародним стандартам і міжнародним зобов'язанням нашої держави у сфері забезпечення та захисту прав і свобод людини і громадянина. Положення Основного Закону відображають основні принципи, що закріплені у Загальній декларації прав людини 1948 р. Зокрема, що “всі люди народжуються вільними і рівними у своїй гідності та правах” (ст.1). У ст. 2 наголошується на рівності прав і свобод, незалежно від “раси, кольору шкіри, статі, мови, релігії, політичних або інших переконань, національного чи соціального походження, майнового, станового або іншого становища” [18]. Конституція України також відповідає положенням Міжнародному пакту про економічні, соціальні та культурні права 1966 р., Міжнародному пакту про громадянські та політичні права 1966 р.

Рівність прав і свобод громадян забороняє будь-якого виду дискримінації і це означає, що держава зобов'язана надати людині засоби дієвого захисту проти будь-якої дискримінації. Водночас, відповідно до Рішення Конституційного Суду України від 7 липня 2004 року № 14-рп/2004, конституційний принцип рівності не виключає можливості законодавця при регулюванні трудових відносин встановлювати певні відмінності у правовому статусі осіб, які належать до різних за родом і умовами діяльності категорій, у тому числі вводити особливі правила, що стосуються підстав і умов заміщення окремих посад, якщо цього вимагає характер професійної діяльності [19]. Не може вважатися дискримінацією висування особливих кваліфікаційних вимог для зайняття певних посад та здійснення професійної діяльності.

Однак мета встановлення певних відмінностей (вимог) у правовому статусі працівників повинна бути істотною, а самі відмінності (вимоги), що переслідують таку мету, мають відповідати конституційним положенням, бути об'єктивно виправданими, обґрунтованими та справедливими. У протилежному випадку встановлення обмежень на зайняття посади означало б дискримінацію [19].

Вікові обмеження є неприпустимими, наприклад для кандидата на посаду керівника вищого навчального закладу третього або четвертого рівня акредитації таке обмеження не ґрунтується на спеціальних вимогах до праці на цій посаді, і оспорювана норма є дискримінаційною щодо реалізації права на працю, а тому суперечить положенням частин першої, другої статті 43, частин першої, другої статті 24 Конституції України, – зазначає Конституційний Суд України [20].

Сутність принципів невідчужуваності та непорушності прав людини полягає в тому, що можливості людини, які в них відображаються, є неодмінною, закономірною приналежністю кожної людини. Їх виникнення датується моментом її народження і не потребує дозволу, схвалення з боку будь-кого, у тому числі й держави. Жодна людина не може бути позбавлена таких можливостей: без них вона – незалежно від місця, часу й умов її існування – не зможе сформувати, розвинути, проявити себе саме як особистість. Оскільки ніхто не дарує людині її прав та свобод – ані держава, ані якесь інше об'єднання, угруповання, ані та чи інша особа, ані тим більше якась “трансцендентна” або уявна істота, то й відібрати, позбавити їх людину ніхто не може” [21, с. 158 ].

Також невідчужуваність є тією ознакою, яка вказує на те, що права є природними, а не похідними. Якщо відповідно до законодавства права можна позбавитися, то вказане право не є природним. Визнання прав людини у ст. 21 Конституції України не тільки

невідчужуваними, а й непорушними, було намаганням законодавця підкреслити природність основних прав людини. “Права людини та основоположні свободи є невід’ємним правом кожної людини, наданим їй від народження”, – зазначається у п. 2 ч. 2 Декларації та Програми дій Всесвітньої конференції з прав людини, яка відбулася під егідою ООН у Відні у 1993 р. [21, с. 158-159].

Тоді як непорушність прав людини – це “незменшуваність”, “недоторканність” можливостей людини, котрі відбиті в тих чи інших її правах [21, с. 159]. У науковій літературі конкретного визначення “непорушність прав” не дається. Проте можна стверджувати, що законодавець таким чином бажав підсилити позиції прав і захистити їх від непередбаченого законом зазіхання з боку будь-кого. Таким чином під непорушністю основних прав і свобод людини розуміється недопущення неправомірного та необґрунтованого встановлення обмежень вказаних прав, їх нескасовність та міцність їх реального впливу на правовий статус особистості. Тобто право є недоторканим і не може бути в будь-який момент припинено відповідно до закону, іншого нормативного акту чи рішення органів державної влади або самоврядування, за виключенням випадків, передбачених безпосередньо у нормах Конституції та Законах України [22, с. 142].

З поняттями невідчужуваності та непорушності прав людини тісно пов’язані (але не тотожні їм) неприпустимість їх скасування та обмеження.

Відповідно до міжнародних стандартів прав людини, легітимне втручання у права людини (у формі їх обмежень) має відповідати основним вимогам: можливий спосіб обмеження встановлюється виключно конституцією; обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими; закон, що обмежує права людини, повинен носити загальний характер; обмеження мають бути пропорційними та обґрунтованими; вони повинні оптимально досягати легітимної мети з мінімальним втручанням у реалізацію прав або свобод, не порушувати сутнісний зміст відповідного права [23, с. 55].

Згідно з реченням-приписом 1 ст. 64 Конституції України конституційні права і свободи людини і громадянина не можуть бути обмежені, крім випадків, передбачених Конституцією України. Зокрема, не можуть бути обмежені права і свободи, закріплені у статтях 24, 25, 27 – 29, 40, 47, 51, 52 – 63 [1].

Як зазначено в Рішенні Конституційного Суду України від 22 травня 2018 року [23], Верховна Рада України повноважна ухвалювати закони, що встановлюють обмеження, відповідно до таких критеріїв: “обмеження щодо реалізації конституційних прав і свобод не можуть бути свавільними та несправедливими, вони мають встановлюватися виключно Конституцією і законами України, переслідувати легітимну мету, бути обумовленими суспільною необхідністю досягнення цієї мети, пропорційними та обґрунтованими, у разі обмеження конституційного права або свободи законодавець зобов’язаний запровадити таке правове регулювання, яке дасть можливість оптимально досягти легітимної мети з мінімальним втручанням у реалізацію цього права або свободи і не порушувати сутнісний зміст такого права”.

### **Висновки.**

У статті 21 Конституції України закріплено права на свободи та людську гідність, які закріплюються за кожною людиною, незалежно від її конституційно-правового статусу. Ці права є природними та даються людині від народження. Свобода означає реальну можливість вибору, проте ця можливість людини має певні об’єктивні межі, які визначаються природними та соціальними закономірностями, явищами, обставинами, умовами. Рівність усіх людей в їх правах і свободах означає необхідність забезпечення їм рівних правових можливостей як матеріального, так і процесуального характеру для

реалізації однакових за змістом та обсягом прав і свобод. Рівність прав і свобод громадян забороняє будь-якого виду дискримінації і це означає, що держава зобов'язана надати людині засоби дієвого захисту проти будь-які види дискримінації.

Характерною рисою німецької правової доктрини є тлумачення свобод крізь призму прав людини. На відміну від Конституції України, в якій розділ II має назву “Права, свободи та обов’язки людини і громадянина”, в Основному Законі ФРН розділ I визначено як “Основні права”. Термін “свобода” не є чітко визначеним в Основному законі ФРН, скоріше Конституція у формі основних прав стала букетом багатьох свобод. Таким чином, у німецькому праві не має як такого чіткого розмежування на “права і свободи”, як в Україні. Права людини слід розуміти як свободи. Основні права розглядаються як способи (виміри) вільного розвитку особистості. У ФРН широко застосовується стале словосполучення: “права на свободу”, яке виражає сутність та зміст між правами та свободами. Таким чином, свободи користуються правовим статусом основних прав, та закріплюються у формі прав на свободу.

Право на гідність не є чітко закріпленим в Конституції України. Воно закріплено у різних її статтях, водночас ніде не має його деталізованого тлумачення. Відповідно до німецької правової доктрини право на гідність є основоположним для всіх інших груп прав. Гарантія людської гідності (стаття 1 Основного Закону ФРН) означає, що втручання в людську гідність не може бути виправдане й обов’язково являє собою порушення основних прав.

Система прав і свобод у Конституції України побудована таким чином, щоб забезпечити законні інтереси людей, тим самим забезпечити принципи непорушності та невідчужуваності прав. Загалом можемо констатувати, що положення Конституції України відповідає міжнародним стандартам прав людини; у ній закріплено механізм захисту прав та свобод, у тому числі від їх можливого обмеження у результаті зловживання ними з боку окремих осіб.

### Використана література

1. Конституція України: Закон України від 28.06.96 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
2. Конституційне (державне) право зарубіжних країн: навч. посібник / Бесчастний В.М., Філонов О.В., Субботін В.М., Пашков С.М.; за ред. Бесчастного В.М. Київ: Знання, 2008. 467 с.
3. Freiheit. Definition: Was ist “Freiheit”? URL: <https://www.wirtschaftslexikon.gabler.de/definition/freiheit-32648> (дата звернення: 10.03.20).
4. Grundgesetz für die Bundesrepublik Deutschland. URL: <https://www.gesetze-iminternet.de/gg/GG.pdf> (дата звернення: 14.03.2020).
5. Науково-практичний коментар до Конституції України / Петришин О.В., Погорілко В.Ф., Притика Д.М., Рабінович П.М., Савенко М.Д., Святоцький О.Д., Сібільова Н.В., Селівон М.Ф., Семенов В.С. Київ: Видавничий Дім “Ін Юре”, 2003. URL: <https://www.jurisprudence.club/konstitutionnoe-uchebnik/stattya-usi-lyudi-vilni-rivni-svojij-gidnosti-47971.html> (дата звернення: 16.03.2020).
6. Андрусяк Т. Історія політичних та правових вчень: лекції. Київ: Юрінком-Інтер, 1999. 304 с. URL: <http://www.politics.ellib.org.ua/pages-cat-29.html> Київ (дата звернення: 12.03.2020).
7. Данильян О.Г. Тараненко В.М. Філософія: підручник. Харків: Право, 2010. 312 с. URL: <http://www.pidruchniki.ws> (дата звернення: 18.03.2020).
8. Рішення Конституційного Суду України від 01.06.16 р. № 2-рп/2016. URL: <https://www.zakon.rada.gov.ua/laws/show/v002p710-16> (дата звернення: 18.03.2020).
9. Савчин М. Порівняльне конституційне право: навч. посібник. Київ: Юрінком Інтер, 2019. 328 с.

10. Jan Schapp Über Freiheit und Recht, Mohr Siebeck 2008, 285 s.
11. Jan Schapp Methodenlehre und System des Rechts, Mohr Siebeck 2009, 276 s.
12. Jan Schapp Freiheit, Moral und Recht. 2. Auflage. Mohr Siebeck, Tübingen 2017, 319 s.
13. Hans Heinrich Rupp (2006) Einteilung und Gewichtung der Grundrechte. Handbuch der Grundrechte in Deutschland und Europa. Band II / C.F. Muller, Verlagsgruppe Huthing Jehle Rehm GmbH, Heidelberg, Munchen, Landsberg, Berlin. 1548 s.
14. Косілова О.І. Розуміння свободи у працях Бенжамена Констана. *Актуальні проблеми юридичної науки*. Хмельницький: Вид-во Хмельниц. ун-ту упр. та права, 2013. Ч. 1. С.42-44.
15. Скасування та звуження існуючих прав і свобод людини та громадянина. *Місьцеве самоврядування*. 2018. № 7/1. URL: <https://www.i.factor.ua/ukr/journals/ms/2020/february/issue2/1>; <https://www.i.factor.ua/ukr/journals/ms/2018/july/issue-7/1/article-37770.html> (дата звернення: 18.03.2020).
16. BVerfG, Urteil vom 15.02.2006 – 1 BvR 357/05 URL: [https://www.bundesverfassungsgesetz.de/SharedDocs/Entscheidungen/DE/2006/02/rs20060215\\_1bvr035705.html](https://www.bundesverfassungsgesetz.de/SharedDocs/Entscheidungen/DE/2006/02/rs20060215_1bvr035705.html) (дата звернення: 15.03.2020).
17. Рішення Конституційного Суду України від 12.04.12 р. № 9-рп/2012 URL: <https://zakon.rada.gov.ua/laws/show/v009p710-12> (дата звернення: 12.03.2020).
18. Чижмарь К. Реалізація міжнародно-правових стандартів рівноправ'я та охорони жінок у правовій системі України. *Підприємництво, господарство і право*. 2018. № 7. С. 144-149.
19. Загальна декларація прав людини: Резолюція Генеральної Асамблеї ООН від 10 грудня 1948 року № 217. URL: [https://www.old.irs.in.ua/index.php?option=com\\_content&view=article&id=82%3A1&catid=47%3Aun&Itemid=74%E2%8C%A9=ru](https://www.old.irs.in.ua/index.php?option=com_content&view=article&id=82%3A1&catid=47%3Aun&Itemid=74%E2%8C%A9=ru) (дата звернення: 10.03.2020).
20. Рішення Конституційного Суду України від 07.07.04 р. № 14-рп/2004. URL: <https://www.zakon.rada.gov.ua/laws/show/v014p710-04> (дата звернення: 15.03.2020).
21. Конституційний Суд України. URL: <http://www.ccu.gov.ua/storinka-knygy/412-mezhi-ta-obme-zhennya> (дата звернення: 15.03.2020).
22. Конституція України: науково-практичний коментар / редкол.: В.Я. Тацій (голова редкол.), О.В. Петришин (відп. секретар), Ю.Г. Барабаш та ін. 2-е вид., переробл. і допов. – (Нац. акад. прав. наук України). Харків: Право, 2011. 1128 с.
23. Кушніренко О.Г., Возгрін С.Ю., Реалізація принципів невідчужуваності та непорушності прав і свобод як конституційно-правова проблема. *Науковий вісник Ужгородського національного університету. Сер. Право*. 2013. Вип. 23. Ч. I. Т. 1. С.142.
24. Косілова О., Поєдинок В. Втручання у права людини в німецькій та українській правових доктринах. *Порівняльно-аналітичне право*. 2019. № 3. С. 5-56. URL: [http://www.pap.in.ua/3\\_2019/13.pdf](http://www.pap.in.ua/3_2019/13.pdf) (дата звернення: 08.03.2020).
25. Рішення Конституційного Суду України від 22.05.18 р. № 5-п/2018. URL: <http://www.ccu.gov.ua/novyna/uhvaleno-rishennya-konstytuciynogo-sudu-ukrayiny-no-5-r2018> (дата звернення: 12.03.2020).

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

УДК 343.627

ЛЕОНОВ Б.Д., доктор юридичних наук, старший науковий співробітник,
головний науковий співробітник Національної академії СБУ.
ORSID: <https://orcid.org/0000-0002-2488-7377>.

ЧУМАК Л.А., кандидат юридичних наук, доцент.

ГРИНЕНКО С.В., національний менеджер проектів програми “Безпека людини”
Координатора проектів ОБСЄ в Україні.

ПРОБЛЕМИ ЗАПОБІГАННЯ СЕКСУАЛЬНІЙ ЕКСПЛУАТАЦІЇ ДІТЕЙ В МЕРЕЖІ ІНТЕРНЕТ: ДОСВІД ЄС

Анотація. У статті аналізується досвід ЄС із запобігання сексуальній експлуатації дітей в Інтернеті. Висвітлюються проблеми боротьби з цим явищем у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи ЄС у сфері забезпечення діяльності із запобігання сексуальному насильству дітей.

Ключові слова: діти, сексуальна експлуатація, ЄС, мережа Інтернет.

Summary. The article analyzes the EU's experience in preventing the sexual exploitation of children on the Internet. The problems of combating this phenomenon in the domestic information space are highlighted. The legislative initiatives of the EU in the field of ensuring the prevention of child sexual abuse are analyzed.

Keywords: children, sexual exploitation, Internet.

Аннотация. В статье анализируется опыт ЕС в обеспечении предотвращения сексуальной эксплуатации детей в Интернет. Освещаются проблемы борьбы с этим явлением в отечественном информационном пространстве. Анализируются законодательные инициативы ЕС в области обеспечения деятельности по предотвращению сексуального насилия детей.

Ключевые слова: дети, сексуальная эксплуатация, сеть Интернет.

Постановка проблеми. Стрімкий розвиток інформаційних технологій та переваги сучасного цифрового світу обумовили виникнення нових загроз в інформаційній сфері. Однією з таких загроз є поширення практики сексуальної експлуатації дітей в Інтернеті, де продовжує зростати кількість матеріалів, що містять сексуальну експлуатацію дітей. Використання новітніх технологічних форм та засобів в Інтернеті призводить до все більшого залучення злочинцями дітей для виготовлення дитячої порнографії.

Зокрема, у соціальних мережах циркулює близько 12 млн. одиниць контенту, що містять дитячу порнографію. За даними ЮНІФ близько 2 млн. дітей використовують в секс-індустрії щороку. В Інтернеті розміщено більше 1 млн. зображень дітей, над якими вчинене сексуальне насильство. Лише деяких з цих дітей впізнано. Кожні 5 хвилин Internet Watch Foundation знаходить в Інтернеті фото чи відео із сексуальним насильством над дитиною (дитяча порнографія), 40 % з них містять зображення дітей молодше десяти років. Орієнтовна вартість он-лайн-трансляції сексуального насильства над дитиною складає 10-20 євро [1]. Наявні дані про поширеність сексуального насильства щодо дітей в Європі свідчать, що кожна п'ята дитина постраждала від тієї чи іншої форми сексуального насильства, часто з важкими наслідками для її фізичного чи психічного здоров'я і розвитку.

За даними фонду Internet Watch Foundation, Україна посідає 7-ме місце у світі за розповсюдженням дитячої порнографії у всесвітній мережі. За даними Інтерполу, український ринок порнографічної продукції оцінюється у 100 млн. доларів на рік [2].

Особливість сексуального насильства над дітьми в Інтернеті полягає в тому, що матеріали із насиллям залишаються в цій мережі та транслюються по всьому світу.

Результати аналізу наукових публікацій. Кримінально-правові та кримінологічні аспекти боротьби з сексуальною експлуатацією дітей стали предметом дослідження таких вітчизняних вчених, як К.Б. Левченко, І.М. Трубавіна [3], І.А. Нестерова [4], О.В. Іваненко, О.В. Швед [5] та ін.

Вагомий внесок у дослідження сексуальної експлуатації дітей в Інтернеті зробили зарубіжні вчені – М.О. Брайєн, М. Сето [6; 8], Дж. Вуд [8], М.Тейлор [7], Р. Хансон [6], М. Ді Майо [9] та інші.

У дослідженнях зарубіжних дослідників з питань сексуальної експлуатації дітей основна увага приділялася матеріалам, пов'язаним із сексуальною експлуатацією дітей чи різним правопорушенням володіння, поширення або виготовлення таких матеріалів [6; 7] з використанням нових технологій для входження в довіру до дитини з метою її розбещення, сексуального домагання або шантажу [8, с. 320]. Відомо, що випадки входження в довіру до дитини з метою її розбещення та сексуального домагання з використанням мережі Інтернет, мають значні відмінності за своїми формами. Як правило, сексуальна експлуатація дитини в мережі Інтернет відповідає різним складам кримінальних правопорушень, зокрема, таким як входження в довіру дитини з метою розбещення (“грумінг”) та сексуальний примус і шантаж дорослих, а також пов'язаним кримінальним правопорушенням, які визначаються в різний спосіб у законодавствах зарубіжних держав [10]. Це ускладнює розуміння цього злочинного явища, що спричиняє труднощі, пов'язані не лише зі збором фактичних даних, але й з визначенням того, який правоохоронний орган (або його підрозділ) має забезпечувати запобігання сексуальній експлуатації дітей в Інтернеті [9].

Безумовно, ці чинники негативно впливають на формування стратегії запобігання сексуальній експлуатації дітей в Інтернеті. Одним із основних чинників, який обмежує здатність оцінювати справжню сутність явища сексуального примусу та шантажу дітей через мережу Інтернет, є відсутність спільних підходів державного та приватного сектору у запобіганні цьому негативному явищу.

Метою статті є обґрунтування національної стратегії запобігання сексуальній експлуатації дітей в мережі Інтернет на базі аналізу позитивного досвіду ЄС.

Виклад основного матеріалу. Сексуальне насильство над дітьми як поняття відбиває весь спектр емпіричної реальності, коли дитина використовується як об'єкт задоволення сексуальних потреб дорослого, і включає фізичне, вербальне або психічне насильство, навіть у випадках, коли дитина не є об'єктом безпосереднього контакту [5]. Таке насильство залишається серйозною транснаціональною проблемою для більшості країн світу. Багато інституцій, у т.ч. міжнародних, залучено до діяльності із запобігання онлайн насильству дітей.

Одним з майданчиків обміну досвідом і вироблення спільних рішень для розв'язання цієї проблеми є Глобальний саміт проти сексуальної експлуатації дітей онлайн в Аддис-Абебі (Ефіопія), який організовано WeProtect у партнерстві з Африканським Союзом та Урядом Великої Британії [11].

Цікавими є дослідження Національного центру з питань зникнення та експлуатації дітей (NCMEC) мотивації правопорушників, використання ними методів соціальної інженерії та маніпулятивної тактики з метою налагодження більш індивідуальних взаємин [12] та індивідуальної профілактики.

Важливість профілактики для ефективного зниження кількості випадків сексуального насильства та сексуальної експлуатації дітей підкреслюється й в

ініціативах ЄС. У 2007 році Рада Європи прийняла Конвенцію про захист дітей від сексуальної експлуатації та сексуального зловживання [1].

Проте розвиток “культури профілактики” цього явища на рівні ЄС продовжується, і практичні підходи у цій сфері країн-членів мають значні відмінності [13].

Узгодженню різних підходів сприяють зусилля представників Європейської багатодисциплінарної платформи для боротьби із сексуальною експлуатацією дітей (Child Sexual Exploitation European Multidisciplinary Platform Against Criminal Threats (EMPACT-Cyber-CSE)), які у 2016 році підготували звіт, де міститься інформація про факти реагування правоохоронних органів та використання спеціальних знань з розслідування згаданих інцидентів [13].

В свою чергу, Європол вже п'ятий рік поспіль продовжує готувати звіти з оцінкою небезпеки організованої злочинності в Інтернеті, необхідної для розробки стратегій боротьби із нею. Одним із найбільших викликів, перерахованих у новому звіті, є сексуальна експлуатація дітей в Інтернеті. У звіті зазначається, що в Інтернеті продовжує зростати кількість матеріалів, що містять сексуальну експлуатацію дітей [14].

Україна з 2012 року є стороною Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Лансаротська конвенція). У своєму першому звіті з виконання Конвенції Лансаротський комітет закликав Україну узгодити своє законодавство з вимогами конвенції із забезпеченням того, що інтереси дитини стоятимуть на першому місці в розслідуваннях і кримінальних провадженнях, пов'язаних із сексуальною експлуатацією та сексуальним насильством над дітьми [15, с. 14].

Конвенцією Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства, зокрема, передбачено, що кожна держава, що підписала цю Конвенцію, вживає необхідних законодавчих заходів для:

1) забезпечення криміналізації за:

надання доступу до дитячої порнографії за допомогою інформаційно-комунікаційних технологій, володіння дитячою порнографією, вербування дітей для участі в порнографічних виставах або спонукання дитини до участі в таких виставах; примушування дитини до участі в порнографічних виставах або отримання користі від цього чи іншого використання дитини із цією метою; свідоме відвідування порнографічних вистав, у яких залучено дітей (ч. 1 ст. 21);

умисне спонукання дитини, спостерігати за сексуальним насильством або діяльністю сексуального характеру, навіть якщо вона не бере в цьому участі (ст. 22);

умисну пропозицію, зроблену дорослою людиною за допомогою інформаційно-комунікаційних технологій, зустрітися з дитиною для скоєння проти неї одного з правопорушень, передбачених цією Конвенцією (ст. 23);

2) забезпечення спеціалізації осіб, підрозділів та служб, що займаються розслідуваннями у сфері боротьби із сексуальною експлуатацією та сексуальним насильством стосовно дітей, або забезпечує навчання відповідних працівників для цих цілей. Такі підрозділи або служби забезпечуються відповідним фінансуванням (ст. 34 Конвенції);

3) забезпечення можливості навчання всіх осіб, яких залучено до провадження, зокрема суддів, прокурорів та адвокатів, з питань, що стосуються прав дитини й сексуальної експлуатації та сексуального насильства стосовно дітей (ст. 36 Конвенції) [16].

Деякі з цих положень певною мірою відображені в законодавстві України та враховані у правозастосовній практиці правоохоронних органів.

У зв'язку з ратифікацією цієї Конвенції Законом України від 14.03.18 р. № 2334-VIII “Про внесення змін до Кримінального кодексу України щодо захисту дітей від

сексуальних зловживань та сексуальної експлуатації” встановлено мінімальний вік статевого повноліття, уточнено коло осіб, які є суб’єктами злочину, передбаченого ст. 155 “Статеві зносини з особою, яка не досягла шістнадцятирічного віку”, ст. 156 “Розбещення неповнолітніх” КК України (у ч. 2 ст. 155 КК України замість кваліфікуючої ознаки “вчинення батьком, матір’ю, особою, яка їх замінює” передбачено нову кваліфікуючу ознаку “вчинення близькими родичами або членами сім’ї, особою, на яку покладено обов’язки щодо виховання потерпілого або піклування про нього, або якщо вони спричинили безплідність чи інші тяжкі наслідки”), а також доповнено ст. 302 “Створення або утримання місць розпусти і звідництва”) КК України такою кваліфікуючою ознакою, як “вчинення із залученням малолітньої дитини” [17].

Водночас, незважаючи на вжиті заходи, в Україні діяльність із запобігання сексуальному насильству в мережі Інтернет не можна визнати достатньою й такою, що відповідає міжнародним стандартам та стандартам Ради Європи.

Недосконалість нормативно-правової бази України у сфері захисту дітей від сексуальної експлуатації була визначена Ланцаротським комітетом у його першому звіті від 4 грудня 2015 року щодо виконання державами Ланцаротської конвенції. За результатами дослідження, проведеного у 2019 році в рамках проекту “Покладемо край онлайновій сексуальній експлуатації та насильству стосовно дітей у Європі” під егідою Департаменту захисту прав дитини Директорату протидії дискримінації Ради Європи, напрацьовані зміни до законів України, що у разі прийняття дозволять наблизити українське законодавство до європейських стандартів.

Такі зміни містяться у законопроекті “Про внесення змін до деяких законодавчих актів щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства” (реєстр. № 3055 від 11.02.20 р.), який, зокрема, передбачає встановити кримінальну відповідальність за: вчинення дій сексуального характеру з особою, яка не досягла шістнадцятирічного віку (нова редакція ст. 155 КК України), домагання дитини для сексуальних цілей (ст. 156-1 КК України), свідоме одержання доступу, придбання, володіння, виготовлення або розповсюдження дитячої порнографії (ст. 301-1), проведення та відвідування видовищного заходу сексуального характеру за участю неповнолітньої особи (ст. 301-2 КК України) [18]. На думку фахівців ГНЕУ Апарату Голови Верховної Ради України законопроект потребує, зокрема, суттєвого доопрацювання у частині криміналізації окремих різновидів злочинної поведінки щодо дитини, а також перегляду у бік пом’якшення санкцій запропонованих ст. 301-1, 301-2 КК України [19].

У 2018 році в Україні здійснено Техніко-економічне обґрунтування тестування моделі Barnahus, основними критеріями якої визначено: 1) судово-медичні допити експерти проводять відповідно до протоколу, що ґрунтується на доказах; 2) достовірність заяв дитини забезпечують відповідні заходи згідно з принципами “належного судочинства”; 3) доступність медичного обстеження для судово-медичної експертизи, а також забезпечення фізичного благополуччя та відновлення дитини; 4) психологічна підтримка та короткотермінові й довготермінові терапевтичні послуги для травмованої дитини та членів сім’ї й опікунів, що не вчиняли насильства; 5) проведення оцінки потреб у захисті жертви та потенційних братів та сестер у сім’ї [20, с. 13].

Ця модель ґрунтується на європейських стандартах якості Barnahus, основна мета яких полягає у забезпеченні діяльності спільної операційної та організаційної структури, яку заохочують на практиці (перешкоджаючи повторному травмуванню з одночасним гарантуванням достовірних свідчень для суду), та в дотриманні прав дітей на захист від усіх форм сексуальної експлуатації. Основний загальний висновок з досліджень в

Україні зводиться до того, що існують обмежені правові і політичні бар'єри для практики відповідно до загальних наскрізних принципів та стандартів. За результатами дослідження визнано, що відсутність достатніх фінансових та кадрових ресурсів для захисту дітей є основною проблемою в Україні [20, с. 28].

З метою привернення увагу до потреби криміналізації грумінгу (підготовку дитини до сексуального насильства, що мотивується бажанням використати її для сексуального задоволення), зберігання та перегляду матеріалів, що зображують сексуальні насильства над дітьми, розробки спрощеного механізму блокування, видалення таких матеріалів хостерами та Інтернет провайдерами, у Верховній Раді України 4 лютого 2020 р. відкрито виставку “Захист дітей в Інтернеті від сексуального насильства” з експонатами, на яких зображені реальні приклади листування дітей зі злочинцями, які змушували їх надсилати інтимні фото та вступати з ними в “доросле” он-лайн-спілкування. З'явився також сайт з інформацією про захист дітей від сексуального насильства в Інтернеті, де міститься рекомендації, як дітям захиститися від сексуального насильства – Stop SEXтинг, а також функціонує “Лінія повідомлення” щодо видалення та блокування такого контенту [2].

Слід згадати й деякі ініціативи Уряду в цьому напрямку. Так, постановою Кабінету Міністрів України “Про реалізацію експериментального проекту із створення “єдиного входу” опрацювання звернень громадян та запитів на публічну інформацію” від 27.11.19 р. № 972 передбачено визначити та впровадити технічні рішення, необхідні для реалізації експериментального проекту із створення “єдиного входу” опрацювання звернень громадян, запитів на публічну інформацію, звернень та повідомлень про/або від осіб, які постраждали від торгівлі людьми, домашнього насильства, насильства стосовно дітей, або про загрозу вчинення такого насильства [21].

На думку експертів з питань сексуальної експлуатації дітей, доцільною є реалізація заходів в рамках системи повідомлень і підтримки із залученням представників різних секторів. Механізми мають використовувати системний підхід у формі перехресних повідомлень за участі різних сторін з урахуванням заохочень повідомлень про підозру в сексуальній експлуатації або сексуальному насильстві [10]. Вбачається, що реалізація такого механізму зумовлює необхідність навчання співробітників кіберполіції заходам з ідентифікації жертв сексуальної експлуатації та запобігання проявам такої експлуатації в мережі Інтернет, а також оснащення їх відповідним технічним обладнанням.

Останні дослідження з питань профілактики сексуального насильства проти дітей в мережі Інтернет свідчать про те, що визначення пріоритетів втручання і профілактики в цій сфері має базуватися на мультидисциплінарному підході з урахуванням медичних аспектів, коли всі причетні зацікавлені сторони стандартизують свою діяльність з чіткими та узгодженими основними цілями та завданнями [22].

Як свідчить досвід ЄС, при реалізації профілактичних програм, які спрямовані проти небезпечних видів поведінки, таких як “секстинг” (інтимне спілкування за допомогою листування або телефонних розмов), вони не сприймаються молоддю, якщо їх погано представлено. Профілактичні програми можуть стати підґрунтям і надавати матеріали для ефективного навчання, але їх необхідно інтегрувати в ширший освітній контекст із належними рівнями обговорення та подальшої підтримки для молодих людей. Що стосується проблеми сексуального насильства та сексуальної експлуатації дітей, існує потреба в розвитку освітніх програм, які враховують, що правопорушення інколи трапляються, і приділяють більше уваги реагуванню на них та врахуванню почуттів жертви [10].

З 1995 року Рада Європи бере активну участь у низці ініціатив, спрямованих на допомогу Україні в її інтеграції до єдиного європейського правового простору. У Плані дій Ради Європи для України на 2018 – 2021 роки зазначається, що Рада Європи надасть допомогу в розробленні комплексної національної стратегії захисту дітей від насильства, особливо сексуального насильства, а також у формуванні в Україні дружнього до дітей та гендерно чуйного механізму міжвідомчого реагування на випадки сексуального насильства над дітьми. Запроваджуватимуться заходи з підвищення спроможності фахівців надавати захист потерпілим і свідкам сексуального насильства, а також методи підвищення інформованості та профілактики в боротьбі зі сексуальним насильством над дітьми в Україні [15].

За результатами вжитих заходів очікується забезпечення узгодження нормативно-правових актів України у сфері прав людини з європейськими стандартами; удосконалення спроможності відповідних національних інстанцій звітувати про випадки дискримінації та проводити ефективне розслідування [15].

На нашу думку, проблема, що розглядається, може бути ефективно вирішена в цілому за підтримки ініціатив, що сприяють комплексному підходу, ключовими елементами якого є: 1) просвітницька робота; 2) юридична профілактика.

Перша включає освітню роботу з різними категоріями населення: з дітьми – шляхом висвітлення спеціальних тем на уроках правознавства та основ життєдіяльності людини; з батьками та спеціалістами.

Друга – юридичний аспект профілактики сексуальної експлуатації дитини включає триаду: а) розвиток правової бази захисту дітей від злочинних посягань, б) правозастосування і практичну діяльність правоохоронних органів; в) правову освіту населення з питань захисту дітей [5].

Серед основних питань, що стосуються боротьби з сексуальною експлуатацією дітей в Інтернеті, на національному рівні виділяються: державно-приватна взаємодія; співпраця з громадянським суспільством у сфері забезпечення боротьби з сексуальною експлуатацією дітей в Інтернеті; посилення технічного та науково-технічного потенціалу підрозділів кіберполіції; взаємодія кіберполіції з питань кібербезпеки та боротьби з сексуальною експлуатацією дітей в Інтернеті з державними органами, науковими установами, навчальними закладами, громадськими об'єднаннями, представниками Інтернет, телеком та ІТ індустрії; співробітництво у цій сфері з іноземними державами, їх правоохоронними органами і спеціальними службами, а також з міжнародними організаціями, які здійснюють боротьбу з сексуальною експлуатацією дітей в кіберпросторі; контроль за законністю заходів із забезпечення боротьби з сексуальною експлуатацією дітей в Інтернеті; визначення масштабу он-лайн-насильства над дітьми в Україні, практичне застосування національного законодавства про захист дітей від усіх форм сексуальної експлуатації та насильства в Інтернеті, розкриття та розслідування злочинів, пов'язаних із сексуальною експлуатацією дітей в Інтернеті, робота з правопорушниками.

Висновки.

В Україні існує потреба в розробленні комплексної національної стратегії захисту дітей від сексуального насильства, на базі якої слід сформулювати ефективні профілактичні програми, зміст яких з урахуванням досвіду країн ЄС має поєднувати різні види втручання з використанням різноманітних методик. Профілактичні програми, які допомагають захистити дітей від небезпеки в середовищі мережі Інтернет, доцільно включати до складу національних шкільних програм.

В рамках відповідної програми основними пріоритетами мають стати: підвищення спроможності фахівців надавати захист потерпілим і свідкам сексуального насильства; підвищення інформованості та удосконалення профілактики сексуального насильства над дітьми в Україні. Особливу увагу слід звертати на роботу з дітьми, які перебувають у вразливих ситуаціях, зокрема тими, хто постраждав від конфлікту, та дітьми під опікою.

Запобігання сексуальній експлуатації дітей в Інтернеті передбачає вирішення завдань: належного оснащення персоналу кіберполіції інструментами і керівництвом з реагування на злочини, пов'язані із сексуальною експлуатацією дітей в Інтернеті; навчання співробітників поліції, як діяти під час запобігання або розслідування злочинів цієї категорії, розширення можливостей суб'єктів державного та приватного сектору у належній ідентифікації жертв сексуальної експлуатації; надання допомоги дітям, які (імовірно або фактично) стали жертвами сексуальної експлуатації, забезпечення отримання дітьми інформації про ризик сексуальної експлуатації та сексуального насильства, а також про засоби самозахисту; створення служби телефонної допомоги або допомоги в мережі Інтернет для надання порад абонентам; реалізація (під регулярним контролем) заходів втручання, спрямованих на запобігання злочинам сексуального характеру щодо дітей; впровадження захисних програм підтримки жертв та їхніх сімей; надання таким жертвам медичної та термінової психологічної допомоги.

У заходах з реалізації цієї програми необхідно приділити увагу тому, який вплив на правопорушення, що пов'язані із сексуальним примусом і шантажем, має власна поведінка дітей і молодих людей в мережі Інтернет з визначенням ризику та вразливості в їхній поведінці, що уможливорюють сексуальний примус та шантаж в мережі Інтернет.

За результатами доопрацювання законопроекту “Про внесення змін до деяких законодавчих актів щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства” (реєстр. № 3055 від 11.02.20 р.) доцільно внести відповідні зміни до КК України, реалізація яких наблизить українське законодавство до міжнародних стандартів забезпечення захисту дитини від сексуальної експлуатації та насильства, дозволить Україні виконати свої міжнародні зобов'язання за Ланцаротською конвенцією.

Використана література

1. Про захист дітей від сексуальної експлуатації та сексуального насильства: Конвенція Ради Європи від 2007 р. URL: <https://www.rm.coe.int/1680471b54> (дата звернення: 01.03.2020).
2. У Верховній Раді відкрилася виставка, присвячена захисту дітей від сексуального насильства в Інтернеті. URL: http://www.komit.rada.gov.ua/news/main_news/povidomlen/73527.html (дата звернення: 01.03.2020).
3. Система захисту дітей від жорсткого поводження: навч.-метод. посібн. / за ред. К.Б. Левченко, І.М. Трубавіної. Київ: Держсоцслужба, 2005. 396 с.
4. Нестерова І.А. Вчинення злочинів, пов'язаних із сексуальною експлуатацією неповнолітніх у туристичному бізнесі: причини, шляхи подолання. *Адвокат*. 2011. № 12 (135). С. 46-49.
5. Швед О.В. Сексуальна експлуатація неповнолітніх як соціальне явище: тенденції і шляхи профілактики: автореф. дис. ... канд. соціол. наук: спец. 22.00.04. Харків, 2006.
6. Seto, M. C., Hanson, R. K., Babchishin, K.M. Contact sexual offending by men with online sexual offenses, *Sexual Abuse. Journal of Research and Treatment*. 2010. Vol. 23. P. 124-145.
7. Taylor, M. and Quayle, E. Internet sexual offending. *The Cambridge handbook of forensic psychology*. Brown, J. M. E., Campbell, E. A. E. Cambridge University Press, New York, 2010. P. 520-526.

8. Seto, M.C., Wood, J.M., Babchishin, K.M., Flynn, S. Online solicitation offenders are different from child pornography offenders and lower risk contact sexual offenders. *Law and Human Behavior*. 2012. Vol. 6. № 4. P. 320.
9. Ді Майо, М.А. Первинна ідентифікація дітей-жертв торгівлі людьми. Київ, 2012. 88 с. URL: <https://www.osce.org/uk/ukraine/93270?download=true> (дата звернення: 01.03.2020).
10. Сексуальний примус та шантаж через мережу Інтернет як вид злочину проти дітей: точка зору правоохоронців. URL: <http://www.europol.europa.eu> (дата звернення: 01.03.2020).
11. Мінцифра обговорила зі світовими лідерами в Ефіопії боротьбу проти сексуальної експлуатації дітей он-лайн. URL: <https://www.thedigital.gov.ua/news/mintsifra-obgovorila-zi-svito-vimi-liderami-v-efiopii-borotbu-proti-seksualnoi-ekspluatatsii-ditey-onlayn> (дата звернення: 01.03.2020).
12. Центр NCMEC, 2016. URL: <http://www.missingkids.org/sextortion> (дата звернення: 01.03.2020).
13. Combating sexual abuse of children. Directive 2011/93/EU. European Implementation Assessment. URL: http://www.europarl.europa.eu/RegData/etudes/STUD/2017/598614/EPRS_STU%282017%29598614_EN.pdf (дата звернення: 01.03.2020).
14. Європол: нові тенденції он-лайн-злочинності. URL: <https://www.radiosvoboda.org/a/europol-cyber-crime/29496631.html> (дата звернення: 01.03.2020).
15. План дій для України на 2018 – 2021 рр. URL: <https://www.rm.coe.int/coe-action-plan-for-ukraine-2018-2021-ukr/1680925bec> (дата звернення: 01.03.2020).
16. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства: Закон України від 20.06.12 р. № 4988-VI. URL: https://www.zakon.rada.gov.ua/laws/show/994_927 (дата звернення: 01.03.2020).
17. Про внесення змін до Кримінального кодексу України щодо захисту дітей від сексуальних зловживань та сексуальної експлуатації: Закон України від 14.03.18 р. № 2334-VIII. URL: <https://www.zaxid.net/news> (дата звернення: 01.03.2020).
18. Про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської Конвенції): проект закону України. URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68122 (дата звернення: 25.03.2020).
19. Висновок ГНЕУ Апарату Голови Верховної Ради України від 16.03.2020 на проект закону про внесення змін до деяких законодавчих актів України щодо імплементації Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства (Ланцаротської Конвенції). URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68122 (дата звернення: 25.03.2020).
20. Захист дітей від сексуальної експлуатації та сексуального насильства. Техніко-економічне обґрунтування тестування моделі Barnahus в Україні від 01.01.18 р. URL: <https://www.rm.coe.int/cvavgu-jan2018-5-ua-web/16807874dc> (дата звернення: 01.03.2020).
21. Про реалізацію експериментального проекту із створення “єдиного входу” опрацювання звернень громадян та запитів на публічну інформацію: Постанова Кабінету Міністрів України від 27.11.19 р. № 972. URL: <https://www.zakon.rada.gov.ua/laws/show/972-2019-%D0%BF> (дата звернення: 01.03.2020).
22. EU Child Online Safety Project – Enhancing police and industry practice. URL: http://www.mdx.ac.uk/_data/assets/pdf_file/0017/250163/ISEC-report-FINAL.pdf (дата звернення: 01.03.2020).

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

УДК 34.037

УХАНОВА Н.С., старший науковий співробітник  
НДІП НАПрН України.  
ORCID: <https://orcid.org/0000-0002-2366-5166>.

## ОСОБЛИВОСТІ ЗАХИСТУ ПРАВ НЕПОВНОЛІТНІХ В ІНФОРМАЦІЙНОМУ ПРОСТОРІ

**Анотація.** У статті здійснено аналіз теоретико-правових засад та проблемних аспектів захисту прав неповнолітніх в інформаційному просторі. Визначено основні положення вітчизняного законодавства, спрямовані на захист прав неповнолітніх від деструктивних інформаційних впливів з боку небезпечного інформаційного середовища. Виявлено основні інформаційні загрози, що зростають у геометричній прогресії інформаційних потоків, що суттєво впливають на інформаційну безпеку неповнолітніх, які мають значно ширший діапазон загроз і ризиків порівняно із повнолітньою особою у зв'язку з їх психофізіологічними, соціальними та іншими особливостями. Окреслено основні напрямки удосконалення законодавства для створення безпечного інформаційного середовища, сприятливого для дитини.

**Ключові слова:** інформація, інформаційна безпека неповнолітніх, інформаційне насильство, неповнолітні в інформаційному просторі.

**Summary.** Theoretical and legal principles and problematic aspects of the protection of the rights of minors in the information space have been analyzed in the article. The main provisions of the domestic legislation aimed at protecting the rights of minors from destructive information influences from the dangerous information environment are determined. The main information threats that increase in the geometric progression of information flows, which significantly affect the information security of minors, which have a much wider range of threats and risks than adults due to their psychophysiological, social and other characteristics. The main directions of improving the legislation to create a safe information environment conducive to the child are outlined.

**Keywords:** information, information security of minors, information violence, minors in the information space.

**Аннотация.** В статье проанализированы теоретико-правовые основы и проблемные аспекты защиты прав несовершеннолетних в информационном пространстве. Определены основные положения отечественного законодательства, направленные на защиту прав несовершеннолетних от деструктивных информационных воздействий. Выявлены основные информационные угрозы, растущие в геометрической прогрессии информационных потоков, которые существенно влияют на информационную безопасность несовершеннолетних и имеют значительно более широкий диапазон угроз и рисков по сравнению с совершеннолетним лицом в связи с их психофизиологическими, социальными и другими особенностями. Определены основные направления совершенствования законодательства для создания безопасного информационного пространства, благоприятного для ребенка.

**Ключевые слова:** информация, информационная безопасность несовершеннолетних, информационное насилие, несовершеннолетние в информационном пространстве.

**Постановка проблеми.** Сучасне суспільство розвивається досить стрімкими темпами, що провокує значні ризики для захисту прав людини в інформаційному просторі. Найменш захищеною категорією громадян є неповнолітні, які доволі часто стають об'єктом інформаційної пропаганди та негативного впливу мас-медіа на формування їх свідомості. При цьому ризики впливу дестабілізуючих інформаційних



технологій в суспільстві виявляються безпосередньо у нівелюванні усталених моральних норм, спотворенні суспільно-культурних цінностей, пропагуванні насильства, жорстокості та ін.

Проблема захисту прав неповнолітніх в інформаційному просторі посилюється також зі зростанням рівня доступу дітей до засобів сучасних технологій, більшість з яких стали доволі буденними у щоденному вжитку (Інтернет, мобільний зв'язок, тощо). Разом з цим ускладнюються і процеси контролю за рухом даних, з метою попередження негативного інформаційного впливу та його наслідків. Зазначене актуалізує дослідження проблем захисту прав неповнолітніх в інформаційному просторі як в Україні, так і у світі в цілому.

У процесі аналізу наукової літератури було виявлено, що найбільш інформативними джерелами у сфері досліджень проблемних аспектів захисту прав неповнолітніх в інформаційному просторі є праці таких науковців як Варивода К.С. [1], Деточенко Л.С. [2], Дзьобань О.П., Пилипчук В.Г. [3], Довгань О.Д. [4], Корж І.Ф. [5], Куницький В.В. [6], Лесько Н.В. [7], Нерсисян Г.А. [8], Припхан І.І., Артемович І.І. [9], Топчій О.С. [10] та ін. Однак, подальшого дослідження потребують питання, пов'язані з розробкою рекомендацій щодо удосконалення системи правового захисту неповнолітніх в інформаційному просторі.

**Метою статті** є удосконалення захисту прав неповнолітніх в інформаційному просторі.

**Виклад основного матеріалу.** Ряд сучасних дослідників [1 – 10] свідчать про досить значний вплив інформації на суспільство, яка поступово перетворюється на його ціннісне ядро, котре включає цивілізаційні норми та цінності. Наведена ситуація виступає наслідком впливу системи чинників, які проявляються в ході розвитку інформаційних технологій. Водночас процеси становлення сучасного інформаційного простору відбуваються під впливом мас-культур, які, на думку науковців, характеризуються значним рівнем проникнення у вітчизняну культуру не властивих їй цінностей за допомогою засобів масової інформації.

Довгань О.Д. [4], Пилипчук В.Г. та Дзьобань О.П. [3], характеризуючи вплив інформаційного простору на неповнолітніх, акцентують увагу на необхідності аналізу негативного впливу, який чиниться засобами масової інформації на них. На думку авторів, у зв'язку з активним використанням молодим поколінням ресурсів мас-медіа сьогодні важливо досліджувати вплив основної маси джерел інформації на молодь.

Корж І.Ф. [5] відзначає, що сучасні реалії пов'язані із необхідністю опрацювання значних масивів інформації, тому організація правового захисту неповнолітніх на сьогодні має враховувати ці обставини. При цьому особливу увагу потрібно приділяти реальній поведінці індивідів та інших суб'єктів права, яка направлена на реалізацію норм інформаційного права в конкретних правовідносинах, а також правовій психології громадян, посадових осіб, їх оцінкам чинного права, діяльності державних органів та мотивам правомірної чи протиправної поведінки. Саме у цих реальних процесах визначається здатність чинного права бути ефективним регулятором інформаційних правовідносин, так само як спроможність держави забезпечувати ефективне управління справами суспільства.

Куницький В.В. [6] стверджує, що чимало прихильників свободи слова, свободи засобів масової інформації обстоюють всездозволеність у традиційних і комп'ютерних мас-медіа, а органи, що контролюють їх продукцію на предмет розпусти, жорстокості і насильства, відносять до органів цензури.

На думку Лесько Н.В. [7], молодь є тією соціальною групою, яка повною мірою використовує ЗМІ та активно отримує через них інформацію різного змісту. Інформаційний простір має одне з провідних місць за силою виховного впливу після сім'ї та школи, будучи каналом інтенсивної соціалізації. Сутність особливостей сприйняття дитини полягає у переважанні емоційного ставлення до об'єктів дійсності за відсутності глибоких знань про них.

Варивода К.С. [1] свідчить, що у наш час особливої гостроти набула проблема інформаційного насильства. Практично у всіх сучасних серіалах, фільмах, і навіть мультфільмах існує відеоінформація, яка прямо чи опосередковано пов'язана з насильством. Термін “телевізійне насильство” давно використовується в науковому лексиконі і об'єднує в собі демонстрацію нанесення ушкодження або збитків персонажам телевізійних програм або фільмів. Існує ряд досліджень, результати яких свідчать, що перегляд сцен насильства в телепередачах і фільмах орієнтує молодь до подальшої агресії. Було доведено, що насильство може стати причиною ініціації підлітків до агресивної поведінки. ЗМІ є також джерелом вульгарної інформації, порнографії. У телебаченні транслюється багато еротичних фільмів, які розбещують, опошлюють сучасну молодь [1].

У доповнення до зазначеного варто навести міркування Деточенко Л.С. [2] який відзначає, що у сфері духовного життя суспільства велику небезпеку становлять ризики, пов'язані з тривалою пропагандою споживацького способу життя і великою кількістю сцен насильства та жорстокості на телебаченні. Неконтрольований Інтернет створює значні загрози для користувачів, в першу чергу дітей та молоді, які пов'язані з пропагандою і поширенням агресивного контенту. Не можна залишити без уваги негативну роль зростаючого впливу на молодь соціальних мереж, оскільки ряд прикладів яскраво свідчать про негативні наслідки “життя в мережі” [2].

Результати опитувань, які наведені у праці Деточенко Л.С. [2] підтверджують, що під впливом ЗМІ у дітей та підлітків розвивається агресивність. Причому найбільшу агресивність формують комп'ютерні ігри та сучасне кіно (Рис. 1).

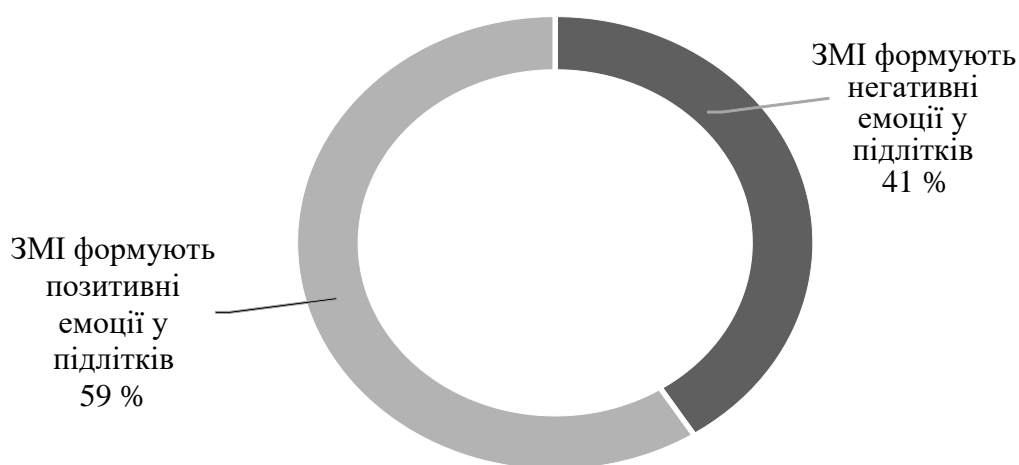


Рис. 1. Ілюстрація результатів опитування щодо впливу ЗМІ на емоції підлітків [2].

Засоби масової інформації впливають на формування у дітей та підлітків негативних почуттів по відношенню до своїх ровесників. Формування образу і стилю життя молоді перебуває під впливом засобів масової інформації, які, на жаль, часто негативно впливають на свідомість і поведінку молодої людини. Це проявляється в

тому, що мас-медіа сьогодні не формують стійких систематичних уявлень молоді про загальні культурно-освітні та правові цінності. Сучасні мас-медіа впливають на спосіб життя молоді

Розкриваючи правові аспекти досліджуваної проблематики варто звернути увагу на нормативно-правові акти, що визначають пріоритети, напрямки та сфери захисту прав неповнолітніх в інформаційному суспільстві. Основними з них є Закони України: “Про охорону дитинства” [11], “Про інформацію” [12], “Про захист суспільної моралі” [13], “Про телебачення і радіомовлення” [14], “Про рекламу” [15] та ін.

Передусім слід зазначити, що 7 листопада 2017 року відповідно до Закону “Про внесення змін до деяких законів України щодо посилення гарантій безпеки дітей” поряд з фундаментальними національними інтересами України, такими як забезпечення державного суверенітету і територіальної цілісності України, охорону дитинства визначено як стратегічний загальнонаціональний пріоритет, *“що має важливе значення для забезпечення національної безпеки України”* [16].

Закон України “Про охорону дитинства” визначає *“обмеження щодо пропаганди артефактів жорстокості та насильства, поширення інформації, яка пригнічує гідність особистості та є чинником загроз для моральної стійкості підлітків та дітей”* [11]. Важливість даного нормативного документу пояснюється необхідністю протидії негативним проявам впливу сучасної інформації, яка висвітлюється у ЗМІ.

У статті 5 Закону України “Про захист суспільної моралі” [13] визначено напрямки роботи органів державної влади у формуванні організаційних, економічних та правових детермінант формування механізмів захисту прав громадян в інформаційному просторі (у тому числі неповнолітніх). Зокрема в Законі акцентується увага на звільнення інформаційного суспільства від елементів, які створюють загрози для морального, інтелектуального та фізичного здоров’я підлітків.

Закон України “Про інформацію” [12] також ідентифікує певні канали та шляхи розповсюдження інформації. Дана інформація може бути джерелом потенційної загрози для неповнолітніх. Тому, логічне продовження положень даного закону відображено у наступному нормативно-правовому акті – Законі України “Про захист суспільної моралі” [13]. Даний документ визначає перелік відповідних заборон щодо формування інформаційного контенту (Рис. 2).

Відповідно до частини 4 статті 20 Закону України “Про охорону дитинства”, визначено умови заборони щодо пропаганди у ЗМІ насильства та жорстокості, розповсюдження порнографії та інформації, що зневажає людську гідність і завдає шкоди моральному благополуччю дитини [11].

Законом України “Про телебачення і радіомовлення” [14] визначено положення про захист інформаційних прав дітей від контенту, який може заважати їх психічному, моральному та фізичному розвитку (ст. 41). Нормативним документом введено заборону на трансляцію ряду телепередач, які містять підозрілий зміст, що може бути предметом інформаційної загрози.

Закон України “Про рекламу” [15] також містить низку статей, що мають забезпечувати неповнолітнім безпечний інформаційний простір. Реклама повинна враховувати особливу чутливість дітей і не завдавати їм шкоди. У рекламі заборонено:

- використання зображень дітей, які споживають або використовують продукцію, призначену тільки для дорослих чи заборонену законом для придбання або споживання неповнолітніми;
- інформацію, яка може підірвати авторитет батьків, опікунів, піклувальників, педагогів та довіру до них дітей;

- заклики до дітей придбати продукцію або звернутися до третіх осіб з проханням зробити покупку;
- використання зображень справжньої або іграшкової зброї, вибухових пристроїв.

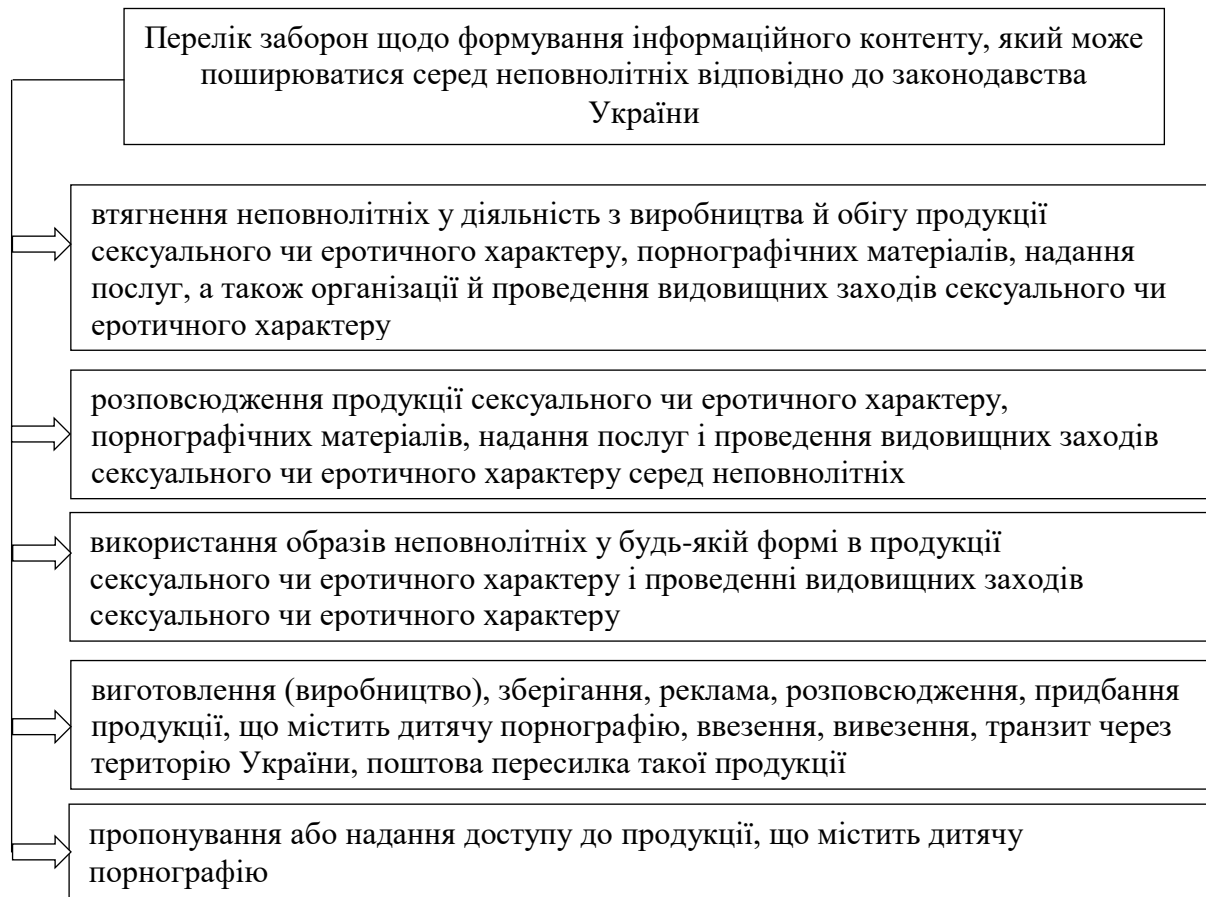


Рис. 2. Основні заборони щодо формування інформаційного контенту, який може поширюватися серед неповнолітніх відповідно до законодавства України [15].

Крім цього, реклама не повинна [15]:

- містити зображення дітей у небезпечних ситуаціях чи за обставин, що у разі їх імітації можуть завдати шкоди дітям або іншим особам;
- містити інформацію, що здатна викликати зневажливе ставлення дітей до небезпечних для здоров'я і життя ситуацій;
- завдавати дітям моральної чи фізичної шкоди, викликати у них відчуття неповноцінності;
- вказувати на можливість придбання рекламованого товару, розрахованого переважно на дітей, кожною сім'єю без урахування можливостей її бюджету;
- створювати у дітей враження, що володіння рекламованою продукцією дає їм перевагу над іншими дітьми.

Аналіз згаданих законів дає підстави стверджувати, що правова протидія негативному впливу інформації на неповнолітніх в Україні зводиться до заборони розповсюдження, використання, виготовлення, зберігання та рекламування продукції, що може бути предметом інформаційної загрози для морального, інтелектуального та фізичного здоров'я неповнолітніх. В Україні немає органу, який би займався моніторингом такої продукції в інформаційному просторі, оскільки створення органів, призначених для контролю продукції мас-медіа зазвичай розцінюється суспільством як цензура.

Законом України “Про внесення змін до деяких законодавчих актів України щодо забезпечення захисту прав дітей” від 21.05.09 р., крім місцевих органів виконавчої влади та органів місцевого самоврядування на *“інші органи виконавчої влади”* в межах їх повноважень покладено обов’язок стосовно подання Кабінету Міністрів України пропозицій щодо вдосконалення положень законодавства, які стосуються забезпечення захисту прав дітей. Ці органи можуть *“подавати висновки до проектів законодавчих актів із зазначених питань та надавати засобом масової інформації, громадськості та особам чи органам, які займаються вирішенням питань захисту дітей, загальну інформацію про забезпечення захисту прав дітей”* [17].

З 17 листопада 2004 р. до 5 березня 2015 року в Україні існував постійний державний експертний і контролюючий орган – Національна експертна комісія України з питань захисту суспільної моралі [18]. Серед основних завдань Комісії – проведення експертизи продукції, що містить елементи або пропаганду культу насильства, жорстокості, порнографії, проведення аналізу процесів і тенденцій, що відбуваються у сфері захисту суспільної моралі, розроблення для органів державної влади та органів місцевого самоврядування рекомендацій з їх правового регулювання та здійснення контролю за дотриманням законодавства у сфері захисту суспільної моралі. Комісією було запропоновано внести зміни до законодавства, якими пропонувалося зобов’язати провайдерів здійснювати контроль українських користувачів в мережі Інтернет, однак запропоновані зміни до законодавства не були схвалені і врешті Комісію взагалі було ліквідовано Постановою Кабінету Міністрів України від 27 травня 2015 року як *“найбільш одіозну державну структуру, яка запам’яталася скандальними рішеннями, спробами заборонити мультфільми про Сімпсонів, пісні Скрибіна та пошуками порнографії у художніх творах”* [19]. Згідно з висновками Міністерства юстиції України, Національна експертна комісія з питань захисту суспільної моралі не мала окремого предмету регулювання і дублювала функції інших державних органів: Міністерства культури і мистецтв України, Міністерства освіти України, Державного комітету телебачення і радіомовлення України, Національну раду України з питань телебачення і радіомовлення та інші.

З цього приводу слід акцентувати увагу на тому, що зазначені органи, в межах своїх повноважень, можуть здійснювати лише опосередкований вплив на інформаційну безпеку неповнолітніх.

Враховуючи зазначене, слід також відзначити, що безпека громадян (у даному випадку дітей) є важливішою, ніж свобода слова. Крім іншого, положення нормативно-правових актів щодо захисту неповнолітніх від негативного впливу інформації не завжди імплементуються у життя з огляду на те, що безпосередньо самі правові норми не здатні забезпечити стійку модель інформаційного простору, яка б враховувала усі нюанси інформаційної безпеки неповнолітніх.

Як зазначає Топчій О.В., значна частина актів, які містять у собі деякі проєкції проблеми, морально застаріла й не відповідає вимогам сьогодення. Більшість розглянутих законів не зовсім вписується у сучасну парадигму епохи інформаційних війн, спеціальних психологічних операцій, не відображає протиріч глобалізаційної доби в контексті негативного впливу на неповнолітніх [10]. Увага законодавця здебільшого сконцентрована на теле-радіосфері, пресі, а не на врегулюванні інформаційних правовідносин у медіапросторі. Внаслідок відсутності чітко артикульованої державної інформаційної політики у досліджуваній галузі залишаються не закріпленими в єдиному джерелі відповідні правові норми і повноваження органів державної влади. В умовах зростання інформаційної агресії, жорсткого протистояння держав з різними установками

на перспективи подальшого розвитку, в тому числі геополітичного, подібна лакуна сама по собі стає загрозою інформаційній безпеці [10].

Куницький В.В. [6] зазначає про наявність певного зв'язку між проявами агресії серед неповнолітніх та впливом сучасних ЗМІ. Автор акцентує увагу на тому, що досить часто генерується інформація, яка здатна створювати ризики для становлення неповнолітнього як особистості. Неадекватна інформація може мати негативний вплив на психіку підлітків, підштовхувати їх до девіантної поведінки. Наведені гіпотези науковця є підтвердженням факту про те, що інформаційні матеріали часто виступають мотиватором молоді у підлітковому віці до негативних вчинків [6].

Отже, для захисту прав неповнолітніх від шкідливого впливу інформації між учасниками медіа-ринку має бути розроблена комплексна стратегія, спрямована проти насильства у ЗМІ. Особи, що відповідають за ЗМІ, мають цілком усвідомлювати свою відповідальність за все, що стосується демонстрації насильства та поширення потенційно шкідливого для дітей контенту, виконуючи при цьому свої обов'язки, пов'язані зі здійсненням права на свободу вираження поглядів. Це може втілюватися шляхом усунення чи блокування доступу до шкідливих матеріалів або через розробку автоматизованих систем класифікації контенту, впровадження механізмів контролю та подання скарг щодо якості контенту тощо [6]. Однак, при запровадженні контролю не слід забувати про такі граничні умови:

- цензура заборонена (ст. 15 Конституції України [20]; закони України у сфері інформаційних відносин);
- кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань (ст. 34 Конституції України) [20];
- кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (ст. 34 Конституції України [20]).

На думку Нерсисяна Г.А. [8], правовий захист дітей від наслідків впливу шкідливого контенту та сприяння їх активній участі в суспільному житті є, насамперед, обов'язком держави. Продуктом такого опрацювання є аналітичні розробки. Потреба в такого виду продуктах обумовила виникнення спеціальних аналітичних структур. Певним аналогом таких структур є традиційні наукові установи. Однак, лише певним. Наукові установи, виготовляючи інформацію найвищої суспільної значимості – наукову інформацію – не мають можливості активно і постійно проявлятися в системі інформаційних обмінів. Задоволення відповідних суспільних потреб було вирішене через створення спеціальних аналітичних структур [8].

Статтею 2 Закону України “Про охорону дитинства” визначено, що завданням законодавства про охорону дитинства, крім іншого, є *“створення правових інститутів з метою захисту прав та законних інтересів дитини в Україні”* [11].

Припхан І.І. та Артемович І.І. пропонують для формування правового механізму захисту неповнолітніх від негативної інформації, що передбачає визначення комплексу правових інструментів, які дозволять нівелювати вплив негативних факторів, які потенційно можуть завдати шкоди розвитку неповнолітніх, створити відповідний позавідомчий орган із орієнтовною назвою “Національний комітет захисту прав неповнолітніх у кіберпросторі”, який би опікувався питаннями державного контролю у сфері захисту неповнолітніх від негативного впливу інформації в мережі Інтернет. На думку науковців, саме цей орган повинен визначати пріоритетні напрямки державної політики у вищезазначеній сфері [9].

У доповнення до зазначеного, Топчій О.С. відзначає, що удосконалення процесів забезпечення інформаційної безпеки неповнолітніх неможливо без врахування досвіду інших країн. Проте сама процедура збирання, обробки, аналізу даних, вироблення пропозицій щодо можливостей адаптації закордонного досвіду, шляхів удосконалення чинного законодавства й проектування нових нормативно-правових документів у напрямі поліпшення процесів забезпечення інформаційної безпеки неповнолітніх є прерогативою науки, зокрема компаративного правознавства. Багатогранність проблеми дає усі підстави вважати, що даний напрям є одним з найперспективніших у дослідженнях в галузі інформаційного права [10].

Для вирішення проблем захисту прав неповнолітніх в інформаційному просторі, на наш погляд, варто значну увагу приділити організаційно-правовим механізмам, які дадуть можливість фільтрувати інформаційний контент. Цю функцію в сучасному світі успішно виконують інформаційно-аналітичні центри, або так звані “фабрики думки”. Положення цих організацій у кожній конкретній державі знаходиться в залежності від багатьох факторів: традицій, політичної культури, рівня розвитку демократичних інститутів, соціально-економічної стабільності та інших елементів конкретної політичної системи. На наш погляд, аналітично-інформаційні центри здатні повністю організувати систему автоматизованого моніторингу будь-якого інформаційного контенту, згідно з вимогами усіх зазначених нормативно-правових документів.

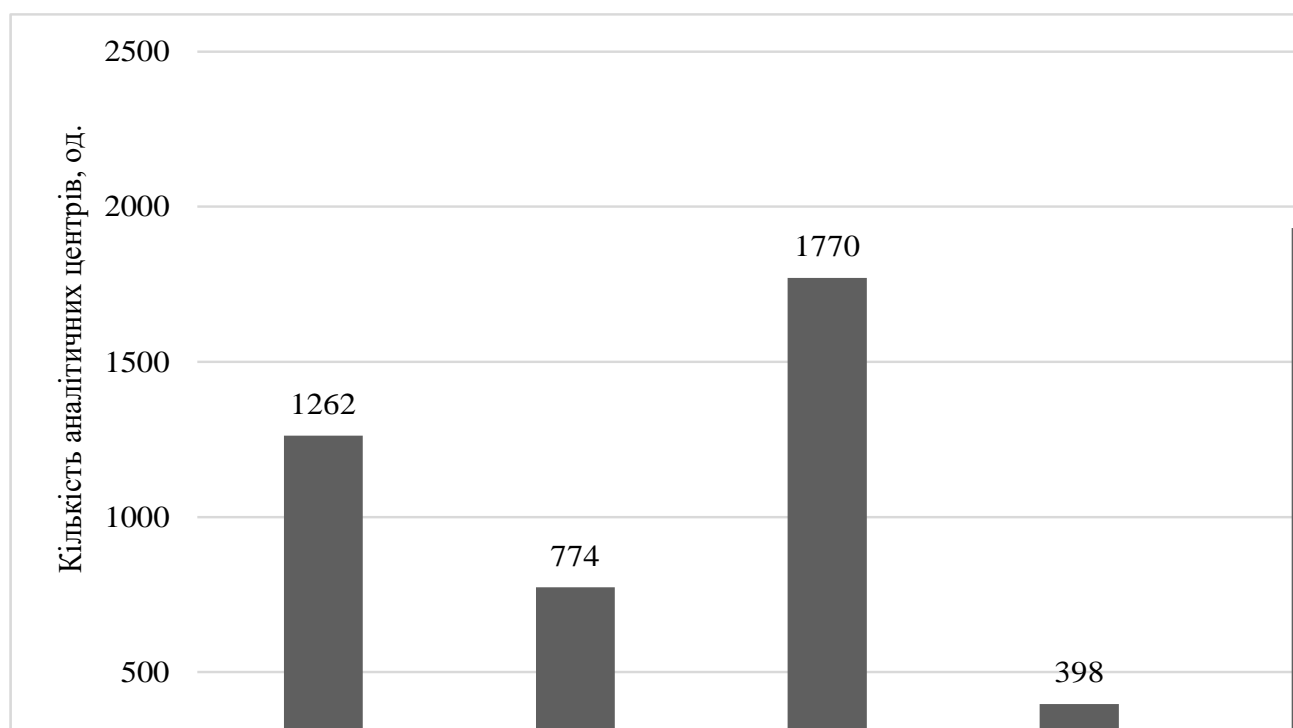


Рис. 3. Кількість аналітичних центрів у сучасному світі, од. [21].

Попит на роботу аналітичних центрів у світі щороку зростає, що пояснюється загальносвітовими глобальними змінами [21]. Кількість аналітичних центрів у світі станом на 2018 рік наведено на Рис. 3. Як свідчать дані рис. 3, найбільша кількість аналітичних центрів сконцентрована в таких регіонах світу як Європа (1770 од.) та Північна Америка (1262 од.). Можна зробити висновки про те, що кількість аналітичних центрів прямо пропорційна розвитку демократичних засад та громадянського суспільства на відповідній території.

Сьогодні робити суттєвий акцент на помітну роль аналітичних центрів в системі організації інформаційної безпеки нашої країни видається передчасним. Однак, зважаючи на перспективу розвитку аналітичних центрів та затребуваність суспільством їх роль зростатиме.

Динаміку кількості аналітичних центрів в Україні наведено на Рис. 4.



Рис. 4. Кількість аналітичних центрів в Україні за період 2016 – 2018 рр., од. [21].

Як свідчать дані Рис. 4, загальна кількість аналітичних центрів в Україні мала поступову тенденцію до зростання упродовж 2016 – 2018 рр., що в цілому позитивно характеризувало основні реформи соціально-політичної системи та трансформацію громадянського суспільства у відповідності до демократичних принципів

З урахуванням зростаючих масштабів проблем сучасної інформаційної безпеки неповнолітніх та зважаючи на все більш чіткі прояви інтеграційних процесів як важливої характеристики сучасного національного розвитку, видається абсолютно логічною думка про необхідність створення в Україні окремої функціональної та організаційної структури в системі національної безпеки з контрольними функціями у сфері інформаційної безпеки неповнолітніх, наприклад, як пропонують Припхан І.І. та Артемович І.І. – “Національний комітет захисту прав неповнолітніх у кіберпросторі”, на який покласти функції державного контролю у сфері захисту неповнолітніх від негативного впливу інформації [9]. Така структура могла б відігравати важливу координаційну роль у сфері інформаційної безпеки для вітчизняних державних і недержавних інформаційних центрів, всієї інформаційної інфраструктури, сприяти утвердженню національної інформаційної політики у внутрішніх і міжнародних обмінах та організації національної інформаційної безпеки в цілому.

#### Висновки.

1. В інформаційному суспільстві формування образу і стилю життя молоді перебуває під впливом засобів масової інформації. На жаль, неконтрольований Інтернет, прихована пропаганда культу насильства, жорстокості, розбещеності, агресивна реклама тощо, сприяє та мотивує неповнолітніх до агресивної поведінки та негативних вчинків.



Мас-медіа, безпосередньо впливаючи на спосіб життя молоді, сьогодні не формують стійких систематичних уявлень молодих людей про загальні культурно-освітні та правові цінності.

2. Правова протидія негативним проявам впливу сучасної інформації на неповнолітніх в Україні спрямована на заборону розповсюдження, використання, виготовлення, зберігання та рекламування продукції, що може бути предметом інформаційної загрози для морального, інтелектуального та фізичного здоров'я підлітків. Відсутність чітко визначеної стратегії убезпечення неповнолітніх від інформаційних загроз, розпорошеність правових норм по широкому колу юридичних актів, відсутність єдиного координуючого та контролюючого органу, значною мірою ускладнює управлінські процеси та унеможливорює належний захист неповнолітніх від інформаційних небезпек.

3. Реалізація права на інформацію у медіапросторі потребує безперервного підтримання стану захищеності неповнолітніх від негативного впливу інформації на свідомість і психіку, що спотворює соціалізацію їх особистості. Усвідомлюючи масштаби цієї проблеми та значення для національної безпеки України, доцільно створити в системі національної безпеки державний орган з контролюючими функціями у сфері захисту неповнолітніх від інформаційних небезпек. Доцільно також вивчити та використати зарубіжний досвід діяльності аналітичних центрів, так званих “фабрик думки”, які можуть стати центральними елементами механізму захисту неповнолітніх від впливу негативної інформації, що поширюється в інформаційному просторі.

4. Забезпечення інформаційної безпеки громадян – це знання і навички, а не лише заборона та блокування небажаного контенту. В багатьох розвинутих країнах значна увага приділяється саме підвищенню освітнього та інтелектуального рівня громадян, що є актуальним і для України.

### Використана література

1. Варивода К.С. Інформаційна безпека підлітків в Інтернет мережі. *Молодий вчений*. 2016. № 3. С. 365-368.
2. Деточенко Л.С. Функции средств массовой информации для молодежной аудитории: по материалам социологического исследования. *Theories and Problems of Political Studies*. 2016. № 5А. С. 35-43.
3. Дзьобань О.П., Пилипчук В.Г. Феномен інформації: історико-правові та філософські аспекти. *Інформація і право*. № 1(13)/2015. URL: <http://ippi.org.ua/pilipchuk-vg-dzoban-op-fenomen-informatsii-istoriko-pravovi-ta-filosofski-aspekti>
4. Довгань О.Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право*. № 2(14)/2015. URL: <http://ippi.org.ua/dovgan-od-suchasni-informatsiini-strukturi-yak-komponenti-informatsiinoi-bezpeki>
5. Корж І.Ф. Об'єкт і предмет наукового дослідження в інформаційній сфері. *Інформація і право*. № 3(22)/2017. С. 22-29.
6. Куницький В.В. Захист неповнолітніх в інформаційному просторі як об'єкт гуманітарної експертизи: український та зарубіжний досвід. *Державне управління: теорія та практика*. 2011. URL: <http://www.academy.gov.ua/ej/ej14/txts/Kunitskiy.pdf>
7. Лесько Н.В. Правове регулювання захисту дітей від негативного впливу Інтернету. *Вісник Національного університету “Львівська політехніка”*. 2016. № 850. С. 48-53.
8. Нерсисян Г.А. Медіаграмотність молоді – запорука протидії інформаційній агресії. *Інвестиції: практика та досвід*. 2018. № 6. С. 56-61.

9. Припхан І.І., Артемович І.І. Правовий механізм захисту неповнолітніх від негативного впливу інформації в мережі Інтернет. *Науковий вісник Ужгородського національного університету*. 2014. № 24. С. 104-108.

10. Топчій О.С. Інформаційна безпека неповнолітніх крізь призму компаративного правознавства. *Інформаційне право*. 2018. № 7. С. 154-158.

11. Про охорону дитинства: Закон України від 26.04.01 р. № 2402-III. URL: <https://zakon.rada.gov.ua/laws/show/2402-14>

12. Про інформацію: Закон України від 02.10.92 р. № 2657-XII URL: <http://zakon1.rada.gov.ua/laws/show/2657-12/ed20110113>

13. Про захист суспільної моралі: Закон України від 20.11.03 р. № 1296-IV. URL: <https://zakon.rada.gov.ua/laws/show/1296-15>

14. Про телебачення і радіомовлення: Закон України від 21.12.93 р. № 3759-XII. URL: <https://zakon.rada.gov.ua/laws/show/3759-12>

15. Про рекламу: Закон України від 03.07.96 р. № 270/96-ВР URL: <https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80>

16. Про внесення змін до деяких законів України щодо посилення гарантій безпеки дітей: Закон України від 07.11.17 р. № 2180-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2180-19#n6>

17. Про внесення змін до деяких законодавчих актів України щодо забезпечення захисту прав дітей: Закон України від 21.05.09 р. № 1397-VI URL: <https://zakon.rada.gov.ua/laws/show/1397-17>

18. Про Національну експертну комісію України з питань захисту суспільної моралі: Постанова Кабінету Міністрів України від 17.11.04 р. № 1550. URL: <https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1550-2004-%EF>

19. Про ліквідацію Національної експертної комісії з питань захисту суспільної моралі: Постанова Кабінету Міністрів України від 27.05.15 р. № 333. URL: <https://zakon.rada.gov.ua/laws/show/333-2015-%D0%BF>

20. Конституція України: Закон України від 28.06.96 р. № 254к/96-ВР URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

21. Світовий рейтинг аналітичних центрів. – (Програма дослідження аналітичних центрів та громадянського суспільства). URL: [http://razumkov.org.ua/images/Material\\_Conference/2017\\_01\\_27/2016\\_Global\\_Think\\_Tank.pdf](http://razumkov.org.ua/images/Material_Conference/2017_01_27/2016_Global_Think_Tank.pdf)

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

Правова інформатика

УДК 316.324.8

ЛАНДЕ Д.В., доктор технічних наук, професор, керівник наукового центру
НДІ інформатики і права НАПрН України.

ПРАВОВІ ПИТАННЯ КОНКУРЕНТНОЇ РОЗВІДКИ

Анотація. У статті викладені правові засади конкурентної розвідки, опис її ролі і місця в сучасному суспільстві, сфер її застосування, стану відповідного правового забезпечення в Україні та світі. Досліджуються основні проблемні питання, пов'язані з керуванням репутацією, захистом комерційної таємниці, персональних даних, авторських прав і суміжних питань. Обґрунтовано актуальність конкурентної розвідки, яка пов'язана з такими процесами, як глобалізація економіки, зростання конкуренції, цифровізація, віртуалізація економіки, розвиток інформаційних технологій. Визначено, що застосування та подальший розвиток правових аспектів конкурентної розвідки може стати важливою ланкою формування сучасного бізнес-середовища.

Ключові слова: конкурентна розвідка, захист комерційної таємниці, захист персональних даних, керування репутацією в мережах, OSINT, відкриті джерела інформації.

Summary. The article is devoted to the legal aspects of competitive intelligence, a description of its role and place in modern society, its application areas, the state of the relevant legal support in Ukraine and the world. The main problematic issues related to reputation management, protection of trade secrets, personal data, copyrights and related issues are investigated. The relevance of competitive intelligence, which is associated with processes such as globalization of the economy, increasing competition, digitalization, virtualization of the economy, the development of information technology, is substantiated.

It is determined that the application and further development of the legal aspects of competitive intelligence can become an important link in the formation of the modern business environment.

Keywords: competitive intelligence, commercial secrets protection, personal data protection, reputation management in networks, OSINT, open information sources.

Аннотация. В статье изложены правовые основы конкурентной разведки, описанию ее роли и места в современном обществе, сферам ее применения, состояния соответствующего правового обеспечения в Украине и мире. Исследуются основные проблемные вопросы, связанные с управлением репутацией, защитой коммерческой тайны, персональных данных, авторских прав и смежных вопросов. Обоснована актуальность конкурентной разведки, которая связана с такими процессами, как глобализация экономики, рост конкуренции, цифровизация, виртуализация экономики, развитие информационных технологий. Определено, что применение и дальнейшее развитие правовых аспектов конкурентной разведки может стать важным звеном формирования современной бизнес-среды.

Ключевые слова: конкурентная разведка, защита коммерческой тайны, защита персональных данных, управление репутацией в сетях, OSINT, открытые источники информации.

Постановка проблеми. Конкурентна розвідка (Competitive Intelligence) охоплює процедури збору і обробки інформації, що проводяться з метою підтримки прийняття управлінських рішень, підвищення конкурентоспроможності комерційних організацій, виключно з відкритих джерел з комп'ютерних мереж [1], більшість з яких є так званими

оверлейними, тобто надбудованими над мережею Інтернет, найпоширеніші з яких – соціальні мережі.

Основна відмінність конкурентної розвідки від бізнес-розвідки в широкому розумінні, в тому числі і від промислового шпигунства – це легітимність і дотримання етичних норм [2]. У конкурентній розвідці це положення доведено до абсолюту – виключно всі джерела інформації повинні бути доступними і легальними.

Очевидно, таке глобальне поняття як конкурентна розвідка вимагає чіткого визначення її легітимних рамок, сфер застосування, правових засад, – цим питанням присвячена ця стаття.

Застосування конкурентної розвідки в комерційній компанії не може бути виправдане тільки міркуваннями інформаційної безпеки, але важливо і для вирішення завдань менеджменту і маркетингу тим, що забезпечує:

- спостереження за репутацією компанії;
- активна участь у формуванні іміджу компанії, інформаційного поля навколо компанії;
- відстеження появи нового конкурента, технології або каналу збуту;
- виявлення можливих злиттів і поглинань;
- оцінка потенційних ризиків при інвестиціях;
- випередження кроків конкурентів в рамках маркетингових кампаній;
- випередження конкурентів в тендерах;
- виявлення каналів витоку інформації.

Хитка грань між поняттями “конкурентна розвідка” і “промислове шпигунство”, полягає в легітимності, законності методів і засобів, що використовуються в процесі збору цільової інформації [3]. Слід зазначити також вельми тонку різницю між бізнес-розвідкою (Business Intelligence) і конкурентною розвідкою. З публікацій і описів систем, де згадуються ці терміни, можна зробити висновок, що бізнес-розвідка спрямована більше на вивчення “внутрішньої” маркетингової, фінансової, економічної інформації та інформації про клієнтів, в той час як конкурентна розвідка частіше охоплює процеси, пов’язані з добуванням “зовнішньої” інформації і знань безпосередньо про конкурентів.

Родоначальником сучасної конкурентної розвідки вважається компанія “Ксерокс”, що зіштовхнулася з конкуренцією з боку японських виробників. У той час японці вийшли на американський ринок з роздрібними цінами нижче собівартості “Ксерокса”. Але “Ксерокс”, завдяки своїй японській філії, створив систему роботи, яку сьогодні називають бенчмаркінгом, засновану на аналізі інформації з відкритих джерел, і отримав успіх.

Приклад нехтування інформації із відкритих джерел. У 70-х роках ХХ століття “Велика трійка” американських виробників автомобілів не прореагувала на появу на ринку японських виробників автомобілів. Однак, самі американці обрали невеликі, економічні і надійні японські автомобілі, і американські корпорації зазнали значних збитків.

Компанія АТ & Т повідомляла, що в неї існує система моніторингу питань, пов’язаних з напрямками діяльності цієї фірми, якими цікавляться співробітники АТ & Т, що працюють в різних регіонах світу. В результаті одного разу новий великий конкурент по одному з видів діяльності АТ & Т був виявлений за місяць до того, як публікації про нього з’явилися у світовій діловій пресі.

В арсеналі тих, хто сьогодні займається конкурентною розвідкою, немає шпигунської техніки. Їх основний інструмент – комп’ютер, підключений до мережі Інтернет, іноді мережевий доступ до спеціальних агрегаторів інформації. Діяльність

сучасних підрозділів конкурентної розвідки компаній часто ґрунтується на останніх досягненнях в області штучного інтелекту, обробки “Великих даних” (Big Data) в поєднанні з напрацюваннями в сферах психології, соціології, економіки.

У цей час створюються численні професійні об’єднання (спільноти) фахівців в галузі конкурентної розвідки. Найбільш відомі з таких спільнот, що займаються організацією конференцій, тренінгів, – це Strategic and Competitive Intelligence Professionals, SCIP ([//www.scip.org](http://www.scip.org)) в США і Competia ([//www.competia.com](http://www.competia.com)) в Канаді.

В Україні відома громадська організація “Спільнота аналітиків і професіоналів конкурентної розвідки” (<https://www.scip.org.ua>). Також ведеться підготовка фахівців в області конкурентної розвідки в Харківському національному університеті радіоелектроніки, де готують магістрів за спеціальністю “Консолідована інформація”.

З початком російської агресії щодо України питання отримання інформації з відкритих джерел і розвінчання фейків отримало нове звучання. Це призвело до старту нових проектів і навчальних платформ, метою яких стало формування і поширення навичок і умінь працювати з інформацією он-лайн, перевіряти інформацію і т.д. Серед таких проектів можна назвати OSINT Academy, сервіс Attack Index (<http://attackindex.com>) і безкоштовний он-лайн курс по OSINT Інституту постіндустріального суспільства [4].

Метою статті є опис поняття конкурентної розвідки, її ролі та місця в сучасному суспільстві в умовах цифровізації, сфер її застосування, дослідження стану відповідного правового забезпечення в Україні та світі, зокрема, основних проблемних питань, пов’язаних із захистом комерційної таємниці, персональних даних, керування репутацією, авторських прав та суміжних питань.

Виклад основного матеріалу

Конкурентна розвідка і OSINT. Методи ведення конкурентної розвідки, техніки і технології її проведення дуже близькі до тих, що використовуються в традиційній розвідувальній діяльності спецслужбами. В англomовній літературі такий вид конкурентної розвідки прийнято називати розвідкою за відкритими джерелами (Open Sources INtelligence, OSINT) [5]. Однак слід зазначити, що OSINT значною мірою обмежена застосуванням у державній, військовій, правоохоронній сфері. Але саме для технологій OSINT створено найбільшу кількість методик, технік, технологій [6; 4; 7].

Комерційна інформація може бути отримана з офіційних джерел, засобів масової інформації, оголошень, реклами, внутрішніх фірмових, банківських, урядових звітів, баз даних, від експертів, шляхом збору, аналізу або спеціальної обробки даних. Відомо, що для бізнес-структур 95 % корисної інформації дає конкурентна розвідка, 4,1 % інформації можна легально отримати від державних структур. Правда, при цьому кількість різномірних відомостей, які необхідно переробити, щоб отримати крупні знання, величезна, а тому в даний час конкурентна розвідка немислима без використання спеціалізованих інформаційних технологій, практичного застосування сучасної концепції “Великих даних”.

Дозволити собі проведення повнофункціональної бізнес-розвідки на ринках можуть тільки великі компанії, проте можливості конкурентної розвідки доступні практично всім.

Значимість розвідки за відкритими джерелами зазначив ще президент США Ліндон Джонсон (Lyndon Baines Johnson) 30 червня 1966 р., коли виголосив промову на церемонії прийняття присяги директором ЦРУ Річардом М. Хелмсом (Richard McGarrah Helms): “Вищі досягнення не є результатом потихеньку переказаної таємної інформації, а впливають з терплячого, повсякчасного вивчення друкованих джерел”.

За твердженнями аналітика ЦРУ Шермана Кента у 1947 р., політики отримують з відкритих джерел до 80 % інформації, необхідної їм для прийняття рішень в мирний час. Пізніше генерал-лейтенант С. Вілсон, який був керівником РУМО США в 1976 – 1977 роках, зазначав, що “90 відсотків розвіданих приходять з відкритих джерел і тільки 10 – за рахунок роботи агентури” [8; 9].

У той же час, аналіз розсекреченого звіту ЦРУ за 1987 рік “Enterprise-Level Computing in Soviet Economy” (SOV C87-10043) дає уявлення про те, який колосальний обсяг даних необхідно було обробляти аналітикам. Для складання звіту постійно протягом року сканували 347 відкритих джерел; для створення зведення обсягом в одну сторінку щодня оброблявся інформаційний масив обсягом приблизно 7 млн. слів.

На державному рівні в США основним правовим механізмом ведення розвідки в відкритих джерелах міністерства оборони є Рада із захисту відкритих джерел (DOSC).

Ця рада консультує і доповідає заступнику міністра оборони з розвідки про питання ведення розвідки в відкритих джерелах, про нові ініціативи щодо поліпшення ефективності роботи підрозділу OSINT і діяльності міністерства оборони в цілому.

В обов’язки ради входять: координація діяльності підрозділу OSINT і ствердження його плану ведення розвідки в відкритих джерелах; визначення послідовності вимог до процесу ведення розвідки в відкритих джерелах.

Армійський стандарт США “АТР 2-22.9” встановлює загальні поняття, основні концепції та методи збору розвідувальних даних з відкритих джерел для Армії США. У цьому документі підкреслюється характеристика OSINT як розвідувальної дисципліни, його зв’язку з іншими розвідувальними дисциплінами, і можливості його застосування в ході спільних операцій.

Використання загальнодоступної інформації є важливим аспектом технічної розвідки (TECHINT). Незважаючи на те, що наміри, можливості і чинники уразливості супротивників і потенційних загроз підлягають засекречуванню, результати OSINT (зокрема, відкритого сервісу “Google Earth”) сприяють отриманню інформації про найбільш потайні держави і організації. Такі приклади свідчать про відповідальність діяльності в цій галузі.

Модель предметної області “Конкурентна розвідка”. Під моделлю предметної області, зокрема, розуміють спеціальним чином сформовану мережу понять, онтологію. Побудова онтології – складна проблема. Перший етап цього процесу – побудова термінологічної основи онтології і визначення семантичних зв’язків.

Нами застосовується методика побудови інформаційних мереж – моделей предметних областей на основі автоматичного моніторингу і аналізу мережевих інформаційних ресурсів довідкового характеру [10]. Як така мережа розглядається мережа понять, що відповідають термінам-заголовкам статей мережевої енциклопедії Wikipedia, що є доступною в мережі Інтернет і не передбачає передплати, крім того, доступна для завантаження у повному обсязі. Для первинного доступу до системи застосовано спеціальний термін Competitive Intelligence (Конкурентна розвідка), за яким існують відповідні статті, що створюються і редагуються експертами-авторами (Рис. 1).

Застосовувався наступний алгоритм побудови моделей предметних областей за даними сервісу Wikipedia [11]:

1. Обирається перший термін-поняття, з якого починається зондування.
2. Відкривається сторінка веб-сервісу (стаття Wikipedia), що відповідає обраному терміну-поняттю. До створюваної мережі додаються всі терміни-поняття, що відповідають гіперпосиланням на обраній сторінці. Формуються ребра-зв’язки до цих вузлів з вихідного вузла.

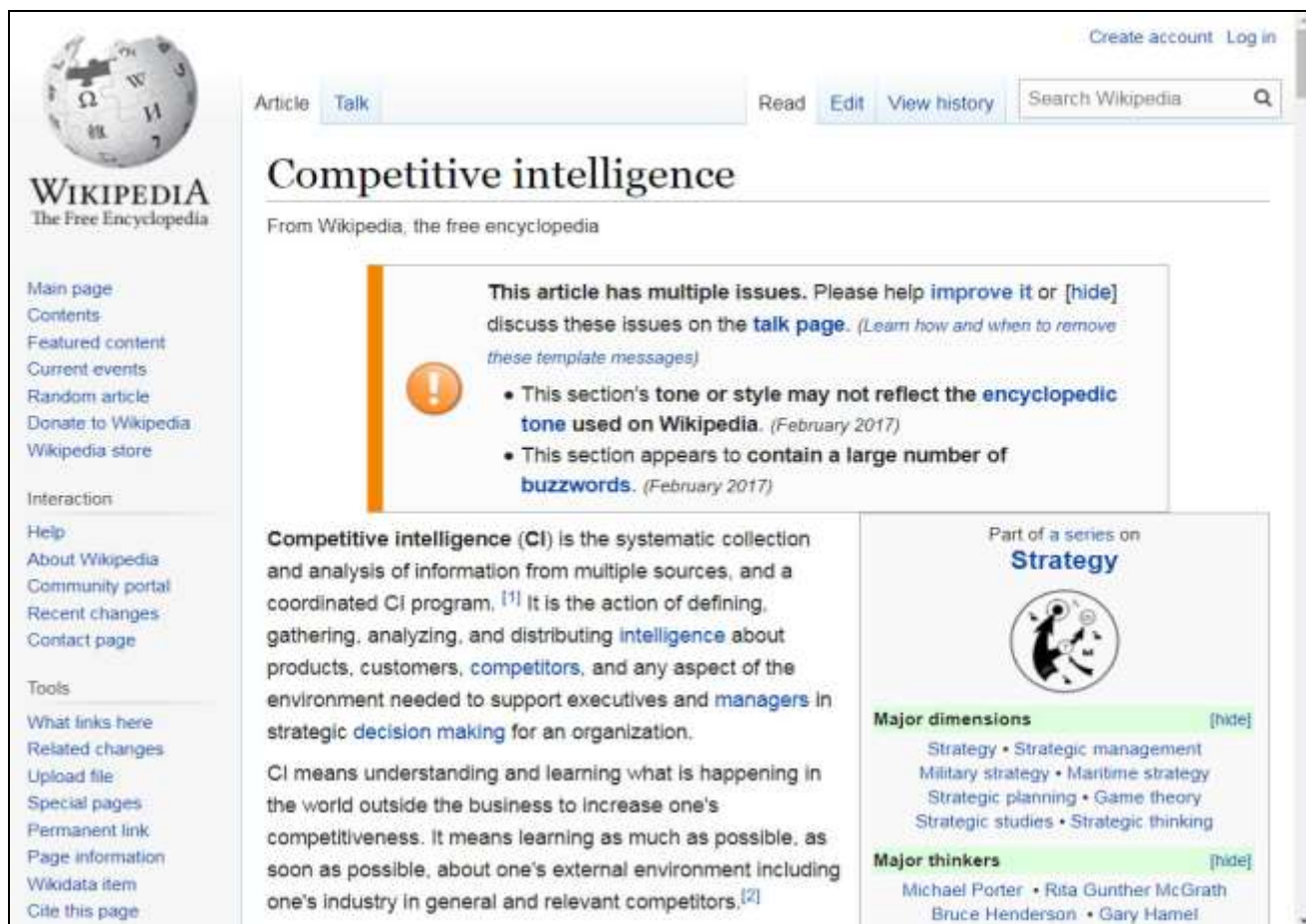


Рис. 1. Інтерфейс користувача системи Wikipedia, розглядається стаття за терміном-поняттям Competitive intelligence

3. Статті, що відповідають гіперпосиланням на попередній сторінці, визначаються як базові, якщо на них міститься гіперпосилання на статтю, що відповідає першому терміну-поняттю, з якого починалось зондування.

4. Із списку вузлів мережі, що формується, визначається той, за яким ще не здійснювалося переходу, на сторінку якого планується перейти для подальшого аналізу. Цей вузол має відповідати вимозі, наведеній у попередньому пункті, та не входить до складу тих вузлів, до сторінок яких вже був здійснений перехід

5. Якщо такий вузол-поняття обрано, то здійснюється перехід до пункту 2.

6. Якщо такого вузла не існує, то вважається, що мережу, що відповідає моделі предметної області, побудовано.

Відповідно до наведеного алгоритму процес збирання інформації з Wikipedia, починаючи з певного вузла-поняття (у нашому випадку – Competitive_intelligence), припиняється, коли відповідно до алгоритму вже неможливий перехід до нового вузла.

Побудовано відповідно до наведеного алгоритму мережі співавторів за базовим терміном-поняттями Competitive intelligence без обмежень на кількість сканованих вузлів. Отримані такі характеристики побудованої мережі: вузлів: 176, зв'язків: 1795, два класи модулярності, дуже висока кластерність: 0.824. Найбільш вагомими за ступенями вузлів поняття наведено у Таблиці 1 (виділені рядки, що містять у словосполученні слово Intelligence).

Таблиця 1. Найбільш вагомі терміни-поняття, що відповідають поняттю Competitive intelligence

| Поняття | Ступень вузла мережі |
|--|----------------------|
| Industrial_espionage | 87 |
| Competitive_intelligence | 83 |
| Business_intelligence | 75 |
| Strategic_planning | 55 |
| University_of_Windsor | 50 |
| SWOT_analysis | 45 |
| Competitor_analysis | 42 |
| Business_war_games | 41 |
| Commercial_intelligence | 41 |
| Marketing_intelligence | 41 |
| Marketing_strategy | 41 |
| Society_of_Competitive_Intelligence_Professionals | 41 |
| Blindspots_analysis | 40 |
| Business_Intelligence | 38 |
| Commercial_Intelligence | 37 |
| Creative_competitive_intelligence | 37 |
| Deformation | 37 |
| Market_intelligence | 37 |
| University_of_Windsor_Faculty_of_Human_Kinetics | 37 |
| Intelligence_analysis | 36 |
| Open_source_intelligence | 35 |
| Media_intelligence | 34 |
| Mercyhurst_College_Institute_for_Intelligence_Studies | 34 |
| Competitor_Intelligence | 32 |
| Corporate_planning | 32 |
| Deloitte_Consulting | 32 |
| OSINT | 32 |
| Global_Intelligence_Forum | 31 |
| Marketing_management | 31 |
| Contify | 30 |
| Mercyhurst_University_Institute_for_Intelligence_Studies | 30 |
| Marketing_analysis | 29 |
| Strategic_and_Competitive_Intelligence_Professionals | 29 |
| Marketing_strategies | 26 |

На Рис. 2 показано приклад процесу виявлення кластерів шляхом застосування спеціального алгоритму, що застосовується в системі Gephi.

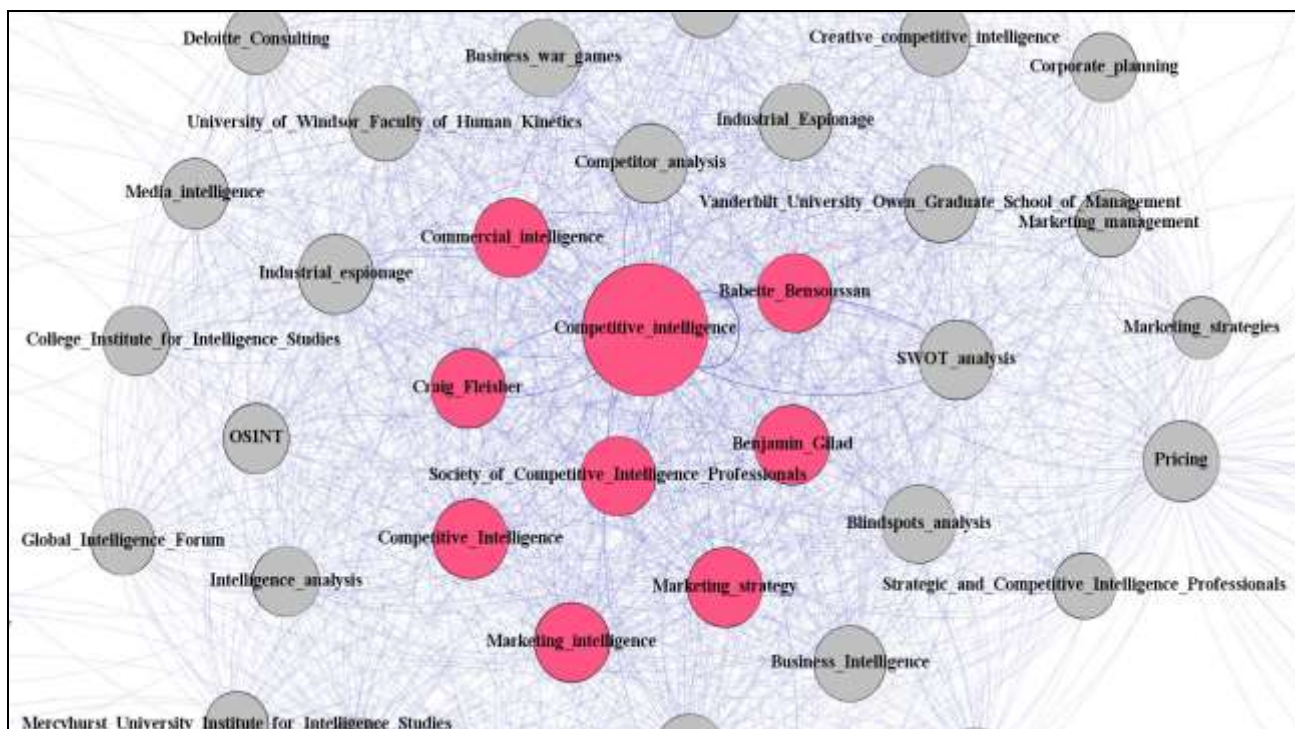


Рис. 2 – Фрагмент моделі предметної області за темою Competitive intelligence

Слід відзначити принципову відмінність запропонованої моделі від існуючих, що базуються на особистій участі експертів при виборі конкретних вузлів і зв'язків. У дослідженні було застосовано лише крипицю знань, представлену у вигляді назви першого, ключового терміну-поняття Competitive intelligence. Після цього програма екстрагувала знання, закладені авторами (редакторами) статей в Wikipedia.

Таким чином, визначено перелік і рівень суміжних до конкурентної розвідки понять, а саме: Business intelligence, Strategic planning, Industrial espionage, Competitor analysis, Commercial intelligence, Marketing intelligence, Marketing strategy, Business intelligence, Commercial intelligence тощо.

Джерела інформації. В інформаційно-аналітичній роботі головною проблемою є знаходження змістовних і загальнодоступних надійних джерел. Коли такі джерела знайдені, застосовуються відповідні технології. Кінцевим інформаційним продуктом аналітичної роботи є знання – синтезовані висновки, рекомендації для прийняття рішень.

Нижче наведено перелік видів інформаційних джерел, які найчастіше використовуються у конкурентній розвідці [12].

1. Прес-релізи компаній, офіційні заяви від імені компаній про нові технології, нові напрямки, угоди, перспективи. Такі прес-релізи створюються компаніями для власної популяризації, залучення уваги потенційних клієнтів, інвесторів, які шукають вигідні варіанти вкладення своїх коштів. Часто в таких заявах є інформація про наміри, події, що плануються. Прес-релізи доступні на веб-сайтах компаній, в PR-службах, на загальних і профільних спеціалізованих майданчиках.

2. Інтерв'ю співробітників компаній, відповідні матеріали в ЗМІ. В інтерв'ю інтерес представляють плани компаній. При цьому з боку служби конкурентної розвідки допускається ініціювання інтерв'ю когось із співробітників об'єкта інтересу.

3. Висловлювання співробітників компаній на форумах, в блогах, в месенджерах, в приватних бесідах. При цьому можуть виявлятися плани компаній, кадрова політика, атмосфера в колективі і т. п. Джерела інформації: 1) Інтернет-ресурси (спеціалізовані форуми, блоги співробітників), блоги експертів, групи в соціальних мережах, месенджерах; 2) виставки, конференції, курси підвищення кваліфікації, професійні заходи.

4. Тендери, закупівлі. Предмети закупівель, обладнання, виконавці. Джерела інформації: 1) Інтернет-ресурси (веб-сайти компаній, торгові майданчики, профільні форуми); 2) партнери досліджуваної компанії, ті, хто брав участь в їх тендерах, у якостях клієнтів і постачальників.

5. Патенти, авторські свідоцтва компанії і її співробітників. Для завдань конкурентної розвідки цікавий їх зміст, спрямованість, списки співавторів. Інформація розміщується на відповідних сайтах (наприклад, [//www.base.ukrpatent.org](http://www.base.ukrpatent.org)). Патентування можливо в будь-якій країні, кращі варіанти – країна реєстрації організації, країна ведення бізнесу, крім того США, Євросоюз, Китай.

6. Розробки компанії: розробки, що ведуться, якими компанія цікавиться. Спостереженню підлягають спроби компанії проводити дослідження: закупівля специфічного обладнання, прийом на роботу фахівців, переговори, відвідування відповідних організацій і т.д.

7. Активність компанії на ринку злиття і поглинань (М & А). Інформація про те, які організації поглинаються, планують поглинути або ведуть переговори про поглинання. Інформацію можна отримати в Антимонопольному комітеті України, за новинним повідомленнями на веб-ресурсах, що присвячені М & А.

8. Вакансії компанії (що відкриваються, закриваються), повідомлення про активний пошук співробітників, вимоги до вакансій, умови. Джерело інформації: веб-сайт компанії, сайти з пошуку роботи та сайти агентств, з якими компанія співпрацює.

9. Інтерес представляє те, чого навчають, яких фахівців запрошують для навчання, які вимоги висувають при залученні слухачів і викладачів, які терміни навчання, яка кількість персоналу навчається.

10. Подяки і нагороди компанії та її співробітників.

11. Участь у заходах (виставки, конференції, круглі столи, презентації). З'ясування, в яких заходах беруть участь компанії, їх спрямованість, коло учасників.

12. Участь в організаціях (союзи, асоціації, спільноти і т.п.) – інформація про те, в яких об'єднаннях бере участь компанія, як активно бере участь, що отримує від участі, на що розраховує, як використовує.

Велика частина цих даних потрапляє в мережеву пресу, прес-релізи або публікується на корпоративних веб-сайтах. Останнім часом великої популярності набувають також бази даних на основі архівів мас-медіа, в тому числі (і переважно) мережевих.

Інформація характеризується якісними, кількісними і ціннісними показниками. До якісних характеристик зазвичай відносять: достовірність, об'єктивність і однозначність інформації. До кількісних характеристик – її повнота і релевантність. Ціннісними характеристиками є вартість і актуальність інформації.

Інтернет за кількістю інформації знаходиться на першому місці у світі, випереджаючи ЗМІ, галузеві видання і одержувані від колег новини, спеціальні огляди, закриті бази даних. При цьому у відкритих джерелах міститься велика частина інформації, необхідна для проведення конкурентної розвідки, однак залишається відкритим питання її знаходження і ефективного використання. Останні дослідження

інформаційного простору показали, що через традиційні інформаційно-пошукові системи доступний трильйон веб-сторінок – це лише “поверхнева видима частина айсберга”. Близько 40 % всієї інформації в Інтернеті є безкоштовною. Навігацію по даному інформаційному простору забезпечують понад мільйон пошукових систем і каталогів, але й вони охоплюють лише малу частину інформаційних ресурсів. Прихованих і невидимих (deeper, invisible) ресурсів мережі Інтернет значно більше – це, перш за все сторінки, що генеруються динамічно, файли різноманітних форматів, інформація з численних баз даних. Сьогодні дуже популярні серед фахівців з конкурентної розвідки бази даних державних і статистичних органів, торговельно-промислових палат, органів приватизації і т.д. Велику користь приносять і окремі доступні бази даних інших органів влади.

Конкурентна розвідка в правовому полі. Конкурентна розвідка як сфера діяльності повинна здійснюватися в рамках правового поля держави. Основою для цього є конституційні права на пошук, отримання, передачу і використання інформації в усіх цивілізованих державах.

Впровадженню систем конкурентної розвідки сприяють законодавчі акти багатьох країн світу. Так, наприклад, в США ще в 1996 році був прийнятий Закон про свободу інформації, який зобов’язав федеральні відомства забезпечити громадянам вільний доступ до всієї своєї інформації. Обмеження стосуються лише матеріалів, що мають відношення до національної оборони, особистих і фінансових документів, а також документів правоохоронних органів.

Однак слід зазначити, що в деяких державах законодавство обмежує подібну діяльність, практично забороняючи конкурентну розвідку.

В Україні “кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір” (Конституція України, Розділ 2, ст. 34). В Україні правове регулювання в інформаційній сфері ґрунтується на наступних принципах:

- 1) свобода пошуку, отримання, передачі, виробництва і поширення інформації будь-яким законним способом;
- 2) встановлення обмежень щодо доступу інформації тільки законами держави;
- 3) відкритість інформації про діяльність державних органів і органів місцевого самоврядування та вільний доступ до такої інформації, крім випадків, встановлених законами держави;
- 4) по категорії доступу інформація поділяється на відкриту (загальнодоступну) і з обмеженим доступом.

Разом з тим, узаконеного поняття “конкурентна розвідка” в Україні сьогодні не існує, хоча діяльність зі збирання, зберігання, обробки та розповсюдження інформації регулюється цілою низкою законодавчих і нормативних актів:

Закон України “Про інформацію” від 02.10.92 р. № 2657-XII (зі змінами від 13.01.11 р.), ст. 5 – 7 [13];

Закон України “Про друковані засоби масової інформації (пресу) в Україні” від 16.11.92 р. № 2782-XII, ст. 6, 25 [14];

Закон України “Про охорону діяльності” від 22.03.12 р. № 4616-VI, ст. 9, 13, 19 [15];

Закон України “Про захист персональних даних” № 2297-VI від 01.06.10 р. [16];

Цивільний кодекс України (ст. 505), Кримінальний кодекс України (ст. 231, 232), Кодекс України про адміністративні правопорушення (ст. 163, ст. 163);

Указ Президента України “Питання європейської та євроатлантичної інтеграції” від 20.04.19 р. № 155/2019 [17];

Указ Президента України “Про Національний Координаційний центр кібербезпеки” від 07.06.16 р. № 242/2016 [18].

Не можна забувати, що здійснення заходів щодо забезпечення безпеки бізнесу навіть в рамках конкурентної розвідки іноді може бути сприйнято як проведення оперативно-розшукової діяльності, проводити яку, відповідно до Закону України “Про оперативно-розшукову діяльність” від 18.02.92 р. № 2135-ХІІ [19] можуть лише суб’єкти, зазначені в окремих статтях даних Законів.

У затвердженій Указом Президента України “Стратегії кібербезпеки України” від 15.03.16 р. № 96/2016 [20] декларуються основні завдання силовим органам, а також передбачається “створення системи своєчасного виявлення, протидії та нейтралізації кіберзагроз, в тому числі із залученням волонтерських організацій”, все це, безумовно, відноситься до застосування засобів конкурентної розвідки в цій галузі.

У той же час чинним Кримінальним кодексом України передбачено кримінальну відповідальність за незаконне збирання з метою використання або використання відомостей, що становлять комерційну таємницю, а також за розголошення комерційної таємниці. Однак такі відомості виходять за рамки конкурентної розвідки.

При досить широкому тлумаченні норм законодавства будь-які процедури збору, обробки та зберігання інформації про конкурентів стають, з одного боку, легітимними, практично безкарними, а, з іншого боку, важко доступними. В Україні фактично закритий доступ до великого пласту вільно доступної в більшості країн інформації, наприклад, щодо нерухомості (наявної і закладеної), земельні ділянки, наявність банківських рахунків і т.п. Більшу частину відомостей можна отримати тільки шляхом консультацій з відповідними експертами.

Як ніколи гостро постала проблема криміналізації окремих служб конкурентної розвідки. Багато служб безпеки сьогодні користуються базами даних з інформацією про людину (тобто, про персональні дані). Такі бази використовуються з цілком благими цілями, наприклад, для перевірки даних про співробітників, партнерів і конкурентів. Очевидно, такими базами даних вони будуть користуватися і надалі, проте будуть вимушені порушувати закон і “йти в підпілля”. Технічно можливості використання і ведення подібних баз даних надають численні системи типу Cronos (оболонки, поширювані цілком легально). За допомогою подібних інструментальних засобів будь-якому зацікавленому користувачу мережі Інтернет стають доступні численні бази даних, які працюють під цими оболонками.

Авторське право. Можна виділити три класи основних проблем авторського права, що мають відношення до конкурентної розвідки. Це проблеми, пов’язані з такими факторами:

- правомірністю використання вхідної інформації (джерел інформації), на підставі якої формуються звіти – результати конкурентної розвідки;
- проблем з авторськими правами на результати конкурентної розвідки;
- правами на застосування (використання) спеціалізованого програмного забезпечення, необхідного для проведення конкурентної розвідки.

Крім того, одна з проблем, що стоїть перед службами конкурентної розвідки в Україні – практично повна відсутність антидемпінгового законодавства.

Ситуація може змінитися, якщо буде створена чітка правова база для конкурентної розвідки.

Авторське право є однією з форм захисту, опублікованих і неопублікованих робіт, передбачених главою 17 Кодексу США, що визначає авторів “оригінальних робіт авторів”, в тому числі літературних, драматичних, музичних і художніх творів. Національні закони про авторські права є обмеженнями конкурентної розвідки. Незважаючи на це, все ж залишаються можливості правомірного використання конкурентної розвідки, що визначається чотирма факторами:

- метою і характером використання;
- властивостями, які використовуються авторських робіт;
- кількістю і частинами авторської роботи, які використовуються;
- впливом використання авторських робіт на потенційний ринок або цінність цих робіт.

Конкурентна розвідка і захист комерційної таємниці. Важливе значення для становлення конкурентної розвідки мав ряд статей Закону України “Про захист від недобросовісної конкуренції” від 07.06.96 р. № 236/96-ВР [21], де (ст. 15-1), забороняється “Неправомірне збирання комерційної інформації”, “Розголошення комерційної інформації”, “Неправомірне використання комерційної інформації” (гл. 4, ст. 16, 17, 19, відповідно).

На цей час українське законодавство про охорону службової та комерційної таємниці являє собою сукупність статей, які містяться в різних правових актах, присвячених в цілому регулюванню інших суспільних відносин.

Поняття комерційної таємниці дано в ст. 505 п. 1 Цивільного кодексу України. Комерційна інформація підлягає захисту, а її втрата може призвести до значних негативних наслідків. Комерційну таємницю яка містить певні рішення, способи, креслення, які часто не можна захистити шляхом отримання охоронних документів, або отримання таких охоронних документів фактично призведе до розкриття інформації, тому таку інформацію суб’єкт господарювання змушений зберігати та охороняти всіма доступними способами. Цивільний кодекс України, визначає комерційну таємницю (ст. 505 п. 1) як інформацію, “яка є секретною в тому розумінні, що вона в загальному або в певній формі та сукупності є невідомою та не легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якого вона належить, у зв’язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів стосовно збереження її секретності, вжитих особою, яка законно контролює цю інформацію”.

Відповідно до цих визначень, як тільки інформація в результаті будь-яких дій потрапляє, наприклад, на сторінки веб-сайту, вона перестає вважатися комерційною таємницею, тому що стає легкодоступною.

Комерційна таємниця віднесена ст. 420 Цивільного кодексу України до об’єктів права інтелектуальної власності.

Хоча в багатьох статтях Кримінального кодексу України (ст. 231, 232, 232-1, 361, 363) встановлено кримінальну відповідальність як за розголошення комерційної таємниці, так і за незаконний збір і використання відомостей, що до неї відносяться, однак, існуюча нормативно-правова база чітко не регламентує, які саме відомості щодо фінансово-господарської діяльності підприємства є комерційною таємницею (за винятком хіба що банківської таємниці, визначення якої дано в ст. 60 Закону України “Про банки і банківську діяльність” [22]).

У Постанові Кабінету Міністрів України “Про перелік відомостей, які не становлять комерційної таємниці” від 09.08.93 р. № 611 визначено цілий клас документів, що стосуються діяльності бізнес-структур, які є фактично відкритими,

зокрема, установчі документи, форми звітності, інформація про участь засновників і посадових осіб в інших компаніях і т.п.

Найчастіше зусилля конкурентної розвідки спрямовані на отримання комерційної таємниці конкурентів. І хоча в різних законодавчих актах даються різні формулювання, можна погодитися з тим [23], що комерційні таємниці характеризуються такою сукупністю ознак: інформація є секретною, є невідомою та не є легкодоступною для осіб, які зазвичай мають справу з видом інформації, до якої вона відноситься; в зв'язку з тим, що є секретною, вона має комерційну цінність. Таким чином, комерційна таємниця – це інформація, яка є корисною і не є загальновідомою. Вона має дійсну або комерційну цінність, з якої можна мати прибуток і для захисту якої власник вживає заходів у всіх сферах життя і діяльності. Таким чином, можна сказати, що діяльність бізнес-розвідки іноді спрямована на видобуток інформації, яка не є загальнодоступною і охороняється законом. Ці діяння порушують величезну кількість статей Кримінального Кодексу України, зокрема, статтю 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю”.

Таким чином, бізнес-розвідка може легітимно використовувати лише ті методи і і способи збору і обробки інформації, що не суперечать законодавству, тобто основні функції конкурентної розвідки – якісний збір, систематизація і, головне, аналіз інформації, а не стеження, підкупи і незаконні хакерські зломи.

Вперше у нас право на збереження комерційної таємниці було проголошено Законом СРСР “Про підприємства в СРСР” від 4 червня 1990 року. У ст. 33 зазначеного Закону розкривалося поняття комерційної таємниці як “відомостей, що не є державними секретами, пов'язані з виробництвом, технологічною інформацією, управлінням, фінансами та іншою діяльністю підприємств, розголошення (передача, витік) яких може завдати шкоди їх інтересам”.

Конкурентна розвідка і захист персональних даних. Приватність, разом з правом на захист життя та свободою слова, є фундаментальними цінностями людства.

Персональні дані, тобто інформація про людей, все більше перетворюється в найдорожчий товар. Така інформація в руках зловмисника – потужна зброя. Державні установи, банки, великі корпорації не завжди можуть забезпечити захист баз персональних даних, які зберігаються у них, в результаті чого, величезний потік конфіденційної інформації надходить на ринок. Тобто персональні дані необхідно захищати.

На сьогодні, основними європейськими правовими стандартами в галузі захисту персональних даних є Конвенція Ради Європи “Про захист осіб у зв'язку з автоматичною обробкою персональних даних” від 28 січня 1981 року (ETS № 108) та “Пакет захисту даних” Європейського Парламенту та Ради від 27 червня 2016 року [24], які є обов'язковими для всіх держав-членів Європейського Союзу і які є предметом для наслідування в області законодавства, в тому числі, і нашою країною. Країни Євросоюзу мають приводити своє законодавство у відповідність зазначеним правовим стандартам.

Ще в 1998 році у Великобританії був прийнятий “Закон про захист персональних даних” – “Data Protection Act 1998”. Його технічна реалізація – проект стандарту “Specification for the management of personal information in compliance with the Data Protection Act 1998” (BS 10012, 2009).

Паралельно з цим свою версію стандарту з безпеки персональних даних випустили в США. Проект документа щодо захисту персональних даних для американських державних структур – “Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)” (SP 800122) регламентує виконання Законів “The Privacy Act of 1974” і “Privacy Protection Act of 1980”.

Канада випустила “Privacy Code” – набір документів для реалізації законодавства щодо захисту відомостей щодо приватних осіб (The Privacy Act і PIPEDA).

У державах-членах Євросоюзу визначення персональних даних, як правило, максимально широкі, в результаті чого громадянами на практиці часто не виконується відповідне законодавство через його зайве “навантаження”. Відповідні органи державної влади, як правило, не роблять ніяких дій, окрім особливих випадків. Важливими залишаються питання виникнення колізій між вимогами приватності та інтересами свободи слова. Сучасними європейськими законами, як правило, забороняється збирання, зберігання, використання та поширення без згоди суб’єкта даних саме критичних персональних даних.

Право на приватність гарантується Конституцією України. Стаття 32 Конституції України говорить: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України”. Крім того в Конституції України передбачений захист ще деяких аспектів приватності. Так, стаття 30 захищає недоторканність житла (територіальна приватність), стаття 31 – таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції (комунікаційна приватність), стаття 32 передбачає заборону збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (інформаційна приватність), а стаття 28 передбачає заборону піддавати особу без її вільної згоди медичним, науковим чи іншим дослідженням (захищаючи елементи фізичної приватності).

Конвенція РЄ про захист осіб у зв’язку з автоматизованою обробкою персональних даних від 28 січня 1981 року (ратифікована Україною 06.07.2010 р.) визначає положення стосовно передачі через національні кордони за допомогою будь-яких засобів персональних даних, що піддаються автоматизованій обробці або зібраних з метою їхньої автоматизованої обробки.

Наступні дані, що часто використовуються для вирішення конкретної особи, означені як особові Управлінням США з менеджменту й бюджету:

- повне ім’я, якщо не поширені (мається на увазі ім’я разом із прізвищем);
- національний ідентифікаційний номер;
- IP-адреса (у деяких випадках);
- номерний знак транспортного засобу;
- номер водійських прав;
- обличчя, відбитки пальців, або почерк;
- номери кредитних карток;
- цифрова ідентичність (цифровий підпис);
- дата народження;
- місце народження;
- генетична інформація.

Згідно із законодавством більшості європейських держав особові дані розділяються за критерієм “чутливості” на дані загального характеру і “чутливі” (вразливі) особові дані.

Загальні особові дані:

- ідентифікаційні дані (прізвище, ім’я, по батькові, адреса, телефон тощо);
- паспортні дані;
- особисті відомості (вік, стать, сімейний стан тощо);
- склад сім’ї;
- освіта;
- професія;

- житлові умови;
- спосіб життя;
- життєві інтереси та захоплення;
- споживчі звички;
- фінансова інформація.

“Чутливі” особові дані:

- інформація про расове, етнічне походження та національність;
- відомості, що стосуються політичних, світоглядних та релігійних переконань;
- відомості про членство в політичних партіях, профспілках, релігійних або громадських організаціях;
- відомості про стан здоров’я і статеве життя;
- генетичні і біометричні дані;
- місце знаходження та шляхи пересування особи;
- інформація щодо застосування до особи заходів в рамках трудового слідства;
- інформація щодо вчинення щодо особи різних видів насильства.

Для з’ясування, яке ж відношення має фізична особа або компанія до захисту персональних даних, велике значення має визначення суб’єктів відносин, пов’язаних із персональними даними (стаття 4 Закону України “Про захист персональних даних” від 01.06.10 р. № 2297-VI): “Суб’єктами відносин, яка пов’язана з персональними даними, є:

- суб’єкт персональних даних;
- власник бази персональних даних;
- розпорядник бази персональних даних;
- третя особа;
- уповноважений державний орган з питань захисту персональних даних;
- інші органи державної влади і органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних”.

В українському законодавстві передбачено повідомний характер обробки персональних даних. Власник або розпорядник (оператор) до початку обробки персональних даних зобов’язаний повідомити уповноважений орган із захисту прав суб’єктів персональних даних про свій намір здійснювати обробку персональних даних. Потім дані про власників або розпорядників (операторів) вносяться до спеціального реєстру операторів. Інформація, що міститься в реєстрі операторів, стає загальнодоступною.

Закони про персональні дані стосуються більшості населення як учасників процесу “обробки” даних. А так як суб’єктом персональних даних є кожна людина, то Закон має загальний характер і стосується кожного. Зокрема, персональні дані широко використовуються в соціальних мережах і сервісах електронної пошти.

Сучасна Інтернет-компанія збирає і обробляє різні категорії персональних даних – своїх співробітників, своїх контрагентів за договорами і деякі дані користувачів своїх сервісів. Люди, що розміщують інформацію про себе в соціальних мережах або службах знайомств, свідомо роблять її відкритою для всіх користувачів ресурсу, і по закону її можна трактувати як “загальнодоступну”, а значить, дотримання особливого режиму конфіденційності щодо її не потрібно, але в соціальних мережах є і інформація, яку користувач приховує, роблячи її доступною тільки для окремої групи користувачів (“друзів”). У цьому випадку Інтернет-ресурс повинен передбачати для неї спеціальні засоби захисту.

Підрозділи конкурентної розвідки займаються обробкою персональних даних, які знаходяться у відкритих джерелах в мережі Інтернет, тобто є загальнодоступними. Для

їх обробки згоди суб'єкта персональних даних не потрібно. Однак при цьому обов'язок доведення, що оброблювані персональні дані є загальнодоступними, покладається на власника або розпорядника. А це означає, що необхідно або накопичувати докази того, що дані взяті з загальнодоступних джерел, або отримувати згоду від суб'єкта персональних даних і потім зберігати цей документ. Крім того, потрібно мати документ, що підтверджує загальнодоступність джерела персональних даних. При цьому залишається без відповіді питання доведеності того, що власник інформаційного ресурсу (веб-сайту) володіє письмовою згодою на обробку.

Правові питання керування репутацією. Одне з важливих завдань конкурентної розвідки – керування репутацією, оцінювання, отримання інформації щодо репутації об'єкту розвідки. Репутація представляє собою соціальну оцінку групи суб'єктів про людину, групу людей або компанії, що сформувалася на основі деяких критеріїв. Репутація компанії – це комплекс оціночних уявлень цільової аудиторії про компанію, сформований на основі факторів репутації, які мають значення для цієї аудиторії. Відповідно до інформаційного листа Вищого господарського суду України “Про деякі питання практики застосування господарськими судами законодавства про інформацію” від 28.03.07 р. ділову репутацію юридичної особи становить престиж її фірмового (комерційного) найменування, торговельних марок та інших належних їй нематеріальних активів серед кола споживачів її товарів та послуг.

Успіх компанії безпосередньо пов'язаний з її репутацією. Так дослідження, проведене австралійськими вченими П. Робертсом і Г. Даулінгом [25], виявило, що чим вище репутація у компанії, тим, по-перше, довше період, протягом якого вона отримує максимальний дохід від своєї діяльності, і, по-друге, тим менше часу компанії потрібно для досягнення середніх по галузі фінансових показників при впровадженні інновацій. Грошовий же еквівалент ділової репутації може бути виражений у формі гудвілу (goodwill). Відповідно до Міжнародних стандартів фінансової звітності (МСФЗ) гудвіл, являє собою різницю між ціною, заплаченою за підприємство покупцями, і “справедливої вартості” (дана величина часто значно відрізняється від простої вартості всіх активів фірми). Наприклад, в правилах бухгалтерського обліку під репутацією розуміється “різниця між купівельною ціною організації та вартістю по балансу всіх її активів і зобов'язань”.

Щоб мати можливість з'ясовувати нематеріальну ціну компанії, розробляються експертні оцінки репутації. Вартість репутації може визначатися експертами, наприклад, таким чином. Спочатку розраховується дохід, отриманий компанією за рахунок бренду, а потім отримана сума множиться на спеціально розрахований коефіцієнт (залежить від положення компанії в галузі, стабільності фінансових показників і т. і.).

Існують і непрямі оцінки рівня репутації компаній, наприклад, засновані на результатах опитування керівників фірм і аналітиків, які оцінюють компанії за такими параметрами, як якість менеджменту і продукту, здатність залучити й утримати кваліфіковані кадри, фінансова стабільність, ефективне використання активів, інвестиційна привабливість, застосування нових технологій і т.п.

Поняття “керування репутацією в Інтернеті” (Online Reputation Management, ORM) по суті являє собою комплекс заходів з виявлення в мережі негативного контенту і зведення його до мінімуму в соціальних медіа і в результатах пошукової видачі. Це, свого роду, PR-кампанія в кіберпросторі. Гілкою ORM є SERM (Search Engine Reputation Management) – пошукове керування репутацією. Зростання ORM в рік у світі в останні роки становить близько 30 %.

Роботи з керування репутацією проводять як спеціалізовані PR-агентства, що працюють на теренах веб-простору, так і підрозділи SEO-агентств, які запускають PR-кампанії, спрямовані на пошук і усунення негативного контенту, співпрацюючи із службами конкурентної розвідки. Основне завдання керування репутацією – формування позитивного іміджу про компанії та її продукти. Зазвичай зусилля концентруються в трьох областях: пошуковій видачі, відгуках в електронних ЗМІ та згадках в соціальних медіа.

Керування репутацією в пошукових системах (Search Engine Reputation Management, SERM) – комплекс заходів, спрямованих на виключення негативних відгуків про компанію, товар або послугу в результатах видачі пошукової системи.

Негативна інформація, що завдає шкоди репутації в мережі, може бути різного походження. Умовно виділяють основні групи походження негативного контенту:

- ненавмисний негатив. Зазвичай такий негатив не представляє великої загрози, але ігнорувати його ні в якому разі не можна;

- умисний негатив з метою вдарити по репутації, наприклад, негативні відгуки звільнених співробітників;

- чорна PR-кампанія – найнебезпечніший вид негативного контенту, що завдає серйозного удару по репутації. Такі PR-кампанії проводять фахівці, які ретельно вивчають бізнес конкурента і точно знають, де прихована ахіллесова п'ята.

Найбільш уразливими тематиками в плані тяжіння негативних відгуків можна назвати:

- банки, фінансові інститути;
- діячі політики і шоу-бізнесу;
- туризм, подорожі (відгуки);
- мобільна техніка і зв'язок;
- побутова техніка;
- заклади громадського харчування.

Відповідно, розміщується і розповсюджується негативний контент на різних майданчиках:

- блоги і форуми;
- соціальні мережі;
- тематичні веб-сайти і портали;
- спеціалізовані сервіси відгуків.

Боротися з негативним контентом покликане пошукове керування репутацією – SERM. Завдання SERM складається у витісненні з результатів пошуку веб-сторінок з небажаною інформацією, в результаті чого цільова аудиторія перестане бачити такі ресурси, так як користувачі не будуть виходити на них за допомогою пошукових систем. Для досягнення цієї мети створюються матеріали з позитивним контентом, припускаючи, що вони витіснять негативні небажані повідомлення. Для розміщення позитивного контенту (з метою витіснення негативного) використовуються найавторитетніші веб-ресурси:

- великі новинні ресурси;
- тематичні портали;
- галузеві форуми;
- персональні блоги та особисті сайти споживачів.

Як простір моніторингу для керування репутацією вибирають мережеві ресурси, де розміщуються відгуки споживачів:

- соціальні мережі, месенджери;

- блоги і форуми;
- тематичні веб-сайти і портали;
- спеціальні сервіси відгуків.

Одним з критеріїв якості послуги моніторингу репутації є повнота охоплення – частка інформації про об'єкт, що досліджується під час роботи від загального обсягу інформації в мережі про об'єкт. Як і раніше основним інструментом пошуку інформації є традиційні пошукові системи, вони охоплюють значну частину Інтернет-контенту, а також деяку частину соціальних медіа.

Висновки.

У роботі було розглянуто поняття конкурентної розвідки, сфер її застосування, правових обмежень і можливостей її застосування. Розглянуті легітимні джерела інформації, а також основні проблемні моменти, пов'язані з питаннями захисту комерційної таємниці, персональних даних, авторських прав та суміжних питань. Розглянуто роль конкурентної розвідки в управлінні репутацією в мережах.

Показано, що актуальність конкурентної розвідки останнім часом значно зросла в усьому світі. Це пов'язано з такими процесами, як глобалізація економіки, зростання конкуренції, цифровізації, віртуалізації економіки, розвиток інформаційних технологій.

Враховуючи тенденції розвитку суспільства і інформаційних технологій, застосування та подальший розвиток правових аспектів конкурентної розвідки може стати основою створення дієвих інструментів формування сучасного бізнес-середовища.

Використана література

1. Додонов А.Г., Ландэ Д.В., Прищепа В.В., Путятин В.Г. Конкурентная разведка в компьютерных сетях. Київ: ИПРИ НАН Украины, 2013. 248 с.
2. Дудихин В.В., Дудихина О.В. Конкурентная разведка в Интернет. Москва: АСТ, НТ Пресс, 2004. 240 с.
3. Ландэ Д., Прищепа В. Школа веб-разведки. Инструменты и источники. *Телеком*. 2007. № 7–8. С. 46-49.
4. Dmytro Lande, Ellina Shnurko-Tabakova. OSINT as a part of cyber defense system. *Theoretical and Applied Cybersecurity*, 2019. № 1. P. 103-108. OSINT Academy. URL: https://www.youtube.com/playlist?list=PL-9OTQQwXf2XuDGO_EIewUOpzUXLDDfcL
5. Берд К. Модель OSINT. *Компьютерра*. 2007. № 22.
6. Army techniques publication FMI 2-22.9. Headquarters Department of the Army Washington, DC, 7 2012.
7. Steele, R.D. Open Source Intelligence: READER Proceedings, 1997 Volume II 6th International Conference & Exhibit Global Security & Global Comp, 1997. P. 329-341.
8. Кондратьев А. На основе открытых источников. *ВПК*. 2009. № 36 (302).
9. Paulson, T.M. Intelligence Issues & Developm. Nova Publishers, 2008.
10. Ланде Д.В. Побудова моделей предметних областей з юриспруденції за даними сервісу Wikipedia. *Інформація і право*. № 4(19)/2016. С. 39-46.
11. Lande D.V., Andrushchenko V.B., Balagura I.V. Formation of the Subject Area on the Base of Wikipedia Service.: материалы междунар. науч.-техн. конф. *Open Semantic Technologies for Intelligent Systems*, г. Минск, 16 – 18 февраля 2017 г. Минск: БГУИР, 2017. Вып. 1. С. 211-214.
12. Нежданов И. Технологии разведки для бизнеса. Москва: Ось-89, 2009. 400 с.
13. Про інформацію: Закон України від 02.10.92 р. № 2657-XII.
14. Про друковані засоби масової інформації (пресу) в Україні: Закон України від 16.11.92 р. № 2782-XII.
15. Про охорону діяльності: Закон України від 22.03.12 р. № 4616-VI.
16. Про захист персональних даних: Закон України від 01.06.10 р. № 2297-VI.

17. Питання європейської та євроатлантичної інтеграції: Указ Президента України від 20.04.19 р. № 155/2019.
18. Про Національний координаційний центр кібербезпеки: Указ Президента України від 07.06.16 р. № 242/2016.
19. Про оперативно-розшукову діяльність: Закон України від 18.02.92 р. № 2135-XII.
20. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”: Указ Президента України від 15.03.16 р. № 96/2016.
21. Про захист від недобросовісної конкуренції: Закон України від 07.06.96 р. № 236/96-ВР.
22. Про банки і банківську діяльність: Закон України від 07.12.00 р. № 2121-III.
23. Основи методики розслідування незаконного збирання та розголошення комерційної таємниці. *Юридичний журнал*. 2006. № 8. С. 48-66.
24. Пилипчук В.Г., Брижко В.М. та ін. 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. С. 37-45.
25. Roberts, P.W., Dowling, G.R. Corporate reputation and sustained superior financial performance. *Strategic Management Journal*. 2002. № 12. P. 1077-1093.

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

---

УДК 681.3, 314.1, 004.6

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

## ПРОБЛЕМА ПЕРСОНАЛЬНИХ ДАНИХ ПРИ ВИКОРИСТАННІ СИСТЕМ ІНТЕРНЕТУ РЕЧЕЙ В ГАЛУЗІ ОХОРОНИ ЗДОРОВ'Я

**Анотація.** В роботі розглядаються можливі механізми неконтрольованої генерації наборів персональних даних системами Інтернету речей при використанні в галузі охорони здоров'я.

**Ключові слова:** інформаційні технології, Інтернет речей, персональні дані, охорона здоров'я.

**Summary.** The paper considers possible mechanisms of uncontrolled generation of personal data sets by the Internet of Things when used in the field of health care.

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

**Аннотация.** В работе рассматриваются возможные механизмы неконтролируемой генерации наборов персональных данных системами Интернета вещей при использовании в области охраны здоровья.

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

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

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

Основною темою при аналізі даної проблеми в наявній літературі є ситуації, пов'язані з безпосереднім отриманням даних за допомогою датчиків ІР та їх можливе несанкціоноване розповсюдження шляхом використання мережних технологій. Зазначимо, що ця тема як така є надзвичайно широкою і містить в собі цілу низку окремих проблем, кожна з яких заслуговує на окреме обговорення.

Однією з них слід вважати доступ до персональних даних громадян системами ІР, які використовуються в галузі охорони здоров'я. В її основі лежить те, що машина може оперувати даними, які вона самостійно збирає та опрацьовує в процесі вирішення задач, що за певних умов можуть виходити за межі стандартного їх набору, передбаченого розробниками та експлуатаційниками. Особливість ситуації полягає в тому, що в медицині (на відміну від більшості інших сфер застосування) системи ІР мають

безпосередній доступ до персональних даних пацієнтів. Маємо на увазі дані, що характеризують стан здоров'я пацієнта і підлягають захисту [9].

В пропонованій роботі ми проаналізуємо принципову здатність систем ІР формувати непередбачені набори даних, які за своєю природою мають бути віднесені до категорії персональних даних. Результатом може бути створення якісно нових комплексів персональних даних, які відсутні в інших наявних джерелах. Такі комплекси утворюються за рахунок поєднання стандартних персональних даних пацієнта, що використовуються працівниками медичного закладу в рамках, передбачених законом, з даними, отриманими шляхом використання різноманітних датчиків. Причому це поєднання здійснює машина без участі (а отже і контролю) людини.

Ми покажемо, що сама природа подібних комплексів даних передбачає необхідність їх зберігання в структурованому вигляді в різноманітних базах даних, що створює значні ризики отримання до них несанкціонованого доступу за допомогою різноманітних мережних технологій. Ситуація ускладнюється тим, що можливість доступу в даному випадку реалізується без відома не лише пацієнта, але й медичного персоналу. Отже питання про відповідальність за наслідки такої можливості є нетривіальним.

**Результати аналізу наукових публікацій.** Правове регулювання в галузі використання технологічних (в тому числі інформаційних) систем саме по собі не є чимось новим.

Мається на увазі правове регулювання відносин між людьми, які здійснюються за допомогою технологічних систем або у зв'язку з їх використанням.

При цьому виділяють дві основні категорії проблем:

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

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

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

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

Загрози та ризики, що виникають в сфері використання ІР, широко обговорюються в експертному середовищі. Стислий виклад поточного стану речей міститься, наприклад в звітах групи Alliance for Internet of Things Innovation, (APII), створеної 2015 року у Європейській Комісії [11]:

- існуюча нормативно-правова база і регуляторні рамки, в основному, відповідають вимогам сучасного цифрового середовища;
- ключ до розвитку ІР полягає у встановленні балансу між гарантуванням безпеки споживачів і стимулюванням інновацій;
- частина ризиків пов'язана з відповідальністю за якість продукції, якій надається особливе значення, хоча вона й застосовує ІР але це не є чимось унікальним для цієї продукції і платформ;
- виникають питання, викликані наявністю відмінності в поняттях “продукт” і “сервіс”, тому необхідні чіткі роз'яснення, щоб уникнути невизначеності;
- забезпечити такий розвиток регуляторної політики, щоб вона була досить гнучкою для можливості врахування схильності промисловості до постійного розвитку, що є для неї ключовим.

Окрему категорію становлять ризики, пов'язані з проблемою захисту персональних даних [7; 8; 12; 13]. ІР за своєю природою орієнтований на збирання великих обсягів даних. Серед них можуть бути і дані, які слід кваліфікувати як персональні.

Важливою є особливість систем ІР, яка полягає в тому, що активне використання великої кількості датчиків створює умови для формування комплексів даних, в тому числі і персональних [14].

Основні аспекти сучасної проблеми захисту персональних даних містяться, наприклад, в матеріалах звіту Федеральної торгової палати США [15]:

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

Галузь охорони здоров'я вважається однією з найперспективніших щодо запровадження технологій ІР [10]. Головна причина полягає в тому, що кількість осіб, що потребують медичних послуг значно перевищує кількість осіб, здатних ці послуги надати. Більше того, пацієнти та потенційні пацієнти розподілені по значних територіях і часто змінюють свою локацію, тоді як медичні заклади централізовані.

Також важливим є те, що сучасна медицина має справу з великим обсягом різноманітних даних, які характеризують стан пацієнта та отримуються з різних джерел, як технологічних, так і “традиційних”.

Основними є такі напрямки використання ІР:

- діагностика;
- моніторинг стану пацієнта;
- лікування пацієнта.

Програмні комплекси здатні не лише отримувати і зберігати дані, але й обробляти їх (підраховувати прогрес від активності, будувати графіки тощо).

Тому можливість використання мережевих технологій для збирання, агрегування, зберігання та опрацювання відповідних даних є вкрай актуальною. Слід також прийняти до відома, що в сучасному світі медицина належить до числа найбільш фінансованих сфер людської діяльності, внаслідок чого виникають сприятливі можливості для різноманітних розробок, зокрема і в галузі ІР.

Аналіз широкого кола джерел свідчить про те, що останнім часом проблема захисту персональних даних у використанні систем ІР активно переходить в сферу прийняття безпосередньо правових рішень [7 – 9].

**Метою статті** є визначення можливих механізмів генерації системами ІР, що працюють в медичній галузі, наборів персональних даних, заснованих на інтеграції стандартних персональних даних пацієнтів з даними, отриманими використовуваними датчиками.

**Виклад основного матеріалу.** Нижче ми проаналізуємо один із аспектів проблеми несанкціонованого поширення персональних даних системами ІР. А саме, принципову здатність систем ІР формувати непередбачені набори даних, які за своєю природою мають бути віднесені до категорії персональних даних. Результатом може бути створення якісно нових комплексів персональних даних, які відсутні в інших наявних джерелах. Такі комплекси утворюються за рахунок поєднання стандартних персональних даних пацієнта з даними, отриманими шляхом використання різноманітних датчиків, які входять до складу систем ІР.

Перш за все зазначимо, що важливою особливістю проблеми персональних даних в медицині є те, що результати роботи датчиків завжди жорстко прив'язуються до конкретної особи, щодо якої передбачене використання її персональних даних. Отже, використання систем ІР неодмінно призведе до формування комплексів даних стосовно конкретної особи. При чому значна частина даних є непередбачуваною, оскільки визначається станом пацієнта, який заздалегідь невідомий. Але саме можливість несанкціонованого використання таких даних і зумовлює головні ризики.

Підкреслимо також, що на наш час саме поняття персональних даних зазнало певного розширення в порівнянні з традиційним розумінням їх як “паспортні дані”. Відповідно до Загального регламенту про захист даних (GDPR), діючого в межах законодавства Європейського Союзу щодо захисту персональних даних, це поняття визначається як “...будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати” [16]. Аналогічно це поняття визначається і Законом України “Про захист персональних даних”.

Для нас в цьому визначенні важливі два моменти:

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

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

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



Також останнім часом до персональних відносять такі специфічні дані:

- файли cookies;
- IP-адреси.

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

В медицині ситуація з персональними даними є досить складною і має специфічні характерні риси. Причина полягає в тому, що в цьому випадку до “стандартних” персональних даних додаються дані іншої природи, що, взагалі кажучи, не є очевидним.

З точки зору чинного законодавства розглядається три категорії даних, що підлягають захисту [9]:

- медична таємниця;
- лікарняна таємниця;
- власне персональні дані.

До медичної таємниці відноситься інформація про

- факт звернення особи за медичною допомогою;
- стан здоров'я особи;
- функціональні особливості організму;
- фізичні недоліки;
- особливості психіки;
- діагноз захворювання особи;
- методи лікування особи;
- інші відомості, включаючи й інформацію про сімейне та інтимне життя.

До лікарняної таємниці відноситься інформація медичного характеру, яка стала відома в зв'язку з виконанням службових обов'язків чи з інших джерел

На перший погляд, перші дві категорії не належать до персональних даних, принаймні в звичайному розумінні. Але вони завжди стосуються особи, яка безперечно є ідентифікованою, а отже (як ми зазначили вище) повинні вважатися персональними даними.

Значна частина подібних відомостей зараз отримується в автоматичному чи автоматизованому режимах шляхом використання відповідних технічних засобів. Більш того, часто в такий самий спосіб здійснюється і первинна обробка отриманих даних. В результаті роботи системи утворюються набори даних, які постійно оновлюються, і заздалегідь неможливо передбачити, яка саме інформація стосовно тієї чи іншої особи буде в них накопичена.

Надання повноцінних медичних послуг передбачає здійснення постійного моніторингу за станом пацієнта. А тому всі дані, що систематично отримуються протягом значних проміжків часу, мають зберігатись у структурованому вигляді в спеціальних базах даних, асоційованих з профілями пацієнтів. Тому йдеться не просто про епізодичне отримання разових даних, а про доступ до конфіденційних баз даних.

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

На рівні технологічної реалізації IP є набором датчиків, що отримують певні дані та пристроїв, що їх обробляють. Для нас суттєво, що обмін даними здійснюється за допомогою мережі Інтернет. Метою створення такої системи є виключення безпосередньої

участі людини принаймні в частині функціональних можливостей системи. Це, в свою чергу означає, що система ІР повинна на основі обробки отриманих вхідних даних приймати рішення, результатом яких буде отримання додаткових даних. Ці додаткові дані можуть мати різні джерела, які більш чи менш строго розподіляються на дві групи:

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

Саме доступність даних другої групи може створювати складні неконтрольовані ситуації. Адже проектувальник системи не може передбачити, запит на які дані сформує машина в певній ситуації, навіть, якщо сама ситуація прогнозована. Прикладом може бути зовнішня система діагностики, яка на підставі певного набору симптомів ставить діагноз хворому. І ця процедура може і не бути передбачена заздалегідь.

Отримання машиною додаткових даних гіпотетично є актуальним для систем з елементами штучного інтелекту [1]. Але у нашому випадку такі ситуації можуть виникати і в значно простіших системах внаслідок, з одного боку, більш вагомої ролі природного інтелекту проектувальників і експлуатаційників, а з другого боку, специфічними особливостями функціонування датчиків, які отримують інформацію, характер якої залежить від багатьох зовнішніх чинників. Прикладом якісно нового елемента даних може бути діагноз, який машина автоматично фіксує на основі “стандартних” показників (температура, тиск, пульс, біохімія крові тощо), які самі по собі змістовного значення не мають і не можуть використовуватися зловмисником у протиправних цілях.

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

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

З точки зору проектувальників, дана система ІР може оперувати персональними даними в обмежених рамках у повній відповідності з існуючими правовими нормами.. Але ми вже казали, що до персональних даних можуть бути віднесені будь-які відомості, так чи інакше пов’язані з тією чи іншою особою. І вони можуть складатися з кількох компонентів. Частина з них передбачена штатним режимом експлуатації системи, а частина – ні.

В медичній сфері також необхідно мати на увазі можливість специфічної форми зловживань, пов’язаних з несанкціонованою модифікацією даних, які використовуються для лікування пацієнтів. Така модифікація може здійснюватись свідомо (наприклад, шляхом зламу системи) з метою завдання шкоди конкретному пацієнту. Зрозуміло, що такі ситуації можливі лише за умови відсутності належного захисту персональних даних пацієнтів.

Такі ситуації породжують додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. І ці загрози можуть становити реальну небезпеку для здоров'я і життя людини.

### **Висновки.**

Отже, ми бачимо, що за певних умов характер функціонування систем ІР в медичній сфері може призводити до використання машиною непередбачених наборів даних, серед яких можуть бути присутні і персональні дані.

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

В результаті виникають додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу обумовлена принциповою неконтрольованістю наборів даних, якими фактично маніпулює машина. Ці загрози ускладнюються тією обставиною, що в сфері медицини вони можуть становити реальну загрозу здоров'ю та життю людини. Отже, виникає необхідність врахування таких загроз при розробці правових норм щодо захисту персональних даних, а також адекватних механізмів реалізації цих норм на практиці.

### **Використана література**

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования: зб. матеріалів II-ї Міжнародної науково-практичної конференції *IT-право: проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ "Львівська політехніка", 2017. 318 с. С. 18-42.
2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений. Структура и функциональные модели архитектуры. Обзор Интернета вещей. URL: <http://handle.itu.int/11.1002/1000/11559>
3. Баранов О.А. "Интернет вещей" як правовий термін. *Юридична Україна*. 2016. № 5-6. С. 96-103. URL: [http://www.irbis-nbuv.gov.ua/cgi-bin/irbis\\_nbuv/cgiirbis\\_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE\\_FILE\\_DOWNLOAD=1&Image\\_file\\_name=PDF/urykr\\_2016\\_5-6\\_16.pdf](http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf)
4. Черняк Л.. Платформа Интернета вещей. *Открытые системы. СУБД*. № 7. 2012. URL: <https://www.osp.ru/os/2012/07/13017643>
5. Kevin Ashton. That 'Internet of Things' Thing. In the real world, things matter more than ideas. *RFID Journal*. 22 June 2009. URL: <http://www.rfidjournal.com/articles/view?4986>
6. Internet of Things. Gartner IT glossary. Gartner. 5 May 2012. "The Internet of Things is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment". URL: <https://www.gartner.com/it-glossary/internet-of-things>
7. Баранов О.А., Брижко В.М. Захист персональних даних в сфері Інтернет речей. *Інформація і право*. № 2(17)/2016. С. 85-91. URL: [http://ippi.org.ua/sites/default/files/11\\_0.pdf](http://ippi.org.ua/sites/default/files/11_0.pdf)
8. Пилипчук В.Г., Брижко В.М. та ін. 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.

9. Булеца С.Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету. Сер. Право*. 2013. Вип. 22. Ч. II. Т. 1. С 186-191. URL: <https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/3366/1/%D0%91%D1%83%D0%BB%D0%B5%D1%86%D0%B0%20%D0%A1.%D0%91.%20%D0%9F%D0%B5%D1%80%D1%81%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D1%96%20%D0%B4%D0%B0%D0%BD%D1%96%20%D0%BF%D0%B0%D1%86%D1%96%D1%94%D0%BD%D1%82%D0%B0%20.pdf>
10. Семанов А.О., Блинников М.А., Пирмагомедов Р.Я. Обзор технологий связи медицинских приложений Интернета вещей. *Информационные технологии и телекоммуникации*. 2018. Т. 6. № 1. С. 63-71. URL: <http://www.sut.ru/doci/nauka/review/20185/63-71.pdf>
11. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels. 28 October 2015. URL: <http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels>
12. Интернет вещей: чем угрожает будущее. URL: <http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee>
13. Как в 2015 году был взломан Интернет вещей. URL: <http://igate.com.ua/news/12342-kak-v-2015-godu-byt-vzloman-internet-veshhej>
14. Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Adopted by the Committee of Ministers on 23 November 2010 at the 1099th meeting of the Ministers' Deputies). URL: [https://search.coe.int/cm/Pages/result\\_details.aspx?ObjectID=09000016805cdd00](https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805cdd00)
15. Internet of Things: Privacy & Security in a Connected. World Federal Trade Commission (FTC) Staff Report. January 2015. URL: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrt.pdf>
16. Про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС: Загальний регламент (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 р. – (В кн. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: зб. документів; пер. з англ. І. Майстренко / за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права НАПрН України). Київ: ТОВ “Видавничий дім “АртЕк”, 2018. 180 с.; URL: <https://gdpr-text.com/?col=2&lang1=ukr&lang2=en&lang3=ruman>

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

Інформаційна і національна безпека

УДК 342.52

МАРУЩАК А.І., доктор юридичних наук, професор.
ORCID 0000-0003-0069-3727.

ПЕТРОВ С.Г., кандидат юридичних наук.
ORCID 0000-0001-7786-4657.

**СУЧАСНИЙ СТАН РОЗВИТКУ НАЦІОНАЛЬНОЇ СИСТЕМИ КІБЕРБЕЗПЕКИ
(НА ПРИКЛАДІ СБ УКРАЇНИ ТА ДЕРЖСПЕЦЗ'ВЯЗКУ УКРАЇНИ)**

Анотація. У статті здійснено аналіз сучасного стану розвитку національної системи кібербезпеки (на прикладі СБ України та Держспецз'язку України). Сформульовано висновок про необхідність врегулювання окремих відносин, пов'язаних з розвитком національної системи кібербезпеки, з урахуванням міжнародної практики. Зокрема, підтримано необхідність врегулювання процедури віднесення до об'єктів критичної інфраструктури, а також незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури. Відзначено, що з визначенням процедури віднесення до об'єктів критичної інфраструктури має запрацювати цілісний правовий механізм як кіберзахисту, так і контррозвідального забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури.

Ключові слова: національна система кібербезпеки, державні електронні інформаційні ресурси, кібербезпека, кіберзахист, інформаційно-телекомунікаційні системи.

Summary. The article deals with the issues of the current state of development of the National Cybersecurity System (on the example of the Security Service of Ukraine and the State Special Service of Ukraine). The conclusion is formulated on the need to regulate certain relations of the National Cybersecurity System development, taking into account international practice. For instance, the need to regulate the procedure for defining critical infrastructure facilities, as well as the independent audit of information security at critical infrastructure facilities, was supported. With the definition of the procedure for classifying objects of critical infrastructure, a holistic legal mechanism should work for both cyber defense and counterintelligence support of cyber security for objects of critical information infrastructure.

Keywords: National Cybersecurity System, state electronic information resources, cybersecurity, cyber defence, information and telecommunication systems.

Аннотация. В статье осуществлен анализ современного состояния развития национальной системы кибербезопасности (на примере СБ Украины и Госспецсвязи Украины). Сформулирован вывод о необходимости урегулирования отдельных отношений, связанных с развитием национальной системы кибербезопасности, с учетом международной практики. В частности, поддержано необходимость урегулирования процедуры отнесения к объектам критической инфраструктуры, а также независимого аудита информационной безопасности на объектах критической инфраструктуры. Отмечено, что с определением процедуры отнесения к объектам критической инфраструктуры должен заработать целостный правовой механизм как киберзащиты, так и контрразведывательного обеспечения кибербезопасности объектов критической информационной инфраструктуры.

Ключевые слова: национальная система кибербезопасности, государственные электронные информационные ресурсы, кибербезопасность, киберзащита, информационно-телекоммуникационные системы.

Постановка проблеми. Служба безпеки України (далі – СБУ) і Державна служба спеціального зв'язку та захисту інформації України (далі – Держспецзв'язку) є одними з основних суб'єктів Національної системи кібербезпеки разом з Національною поліцією України, Міністерством оборони України та Генеральним штабом Збройних Сил України, розвідувальними органами, Національним банком України [1, ст. 8]. Ці два державні органи мають спільну історію у минулому. На даному ж етапі розвитку української державності актуалізуються питання взаємодії СБУ і Держспецзв'язку, зокрема у межах Національної системи кібербезпеки з метою здійснення заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури. У цьому контексті науково-теоретична оцінка сучасного стану та перспектив розвитку Національної системи кібербезпеки на прикладі діяльності СБУ та Держспецзв'язку вбачається нагальною.

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

Частково питання сучасної безпекової політики, зокрема щодо обов'язкового включення до неї питань протидії кіберзброї розкриває Форест Харе [2]. Розвитку національних стратегій кібербезпеки присвячує своє дослідження Петрісор Патраску [3], а найбільш вдало, на нашу думку, компаративістське дослідження стратегій кібербезпеки країн ЄС та НАТО здійснено дослідниками Даріусом Стілісом, Паулісом Пакутінскасом та Інгою Малінаускайте [4]

Однак у цілому питання сучасного стану та перспективи розвитку Національної системи кібербезпеки було предметом наукових досліджень лише фрагментарно.

Метою статті є розкриття сучасного стану розвитку Національної системи кібербезпеки, здійснене на прикладі СБУ та Держспецзв'язку, з акцентом на питання взаємодії зазначених суб'єктів.

Виклад основного матеріалу. Розпочнемо з аналізу норм Закону України “Про Службу безпеки України”, які передбачають взаємодію СБ України з державними органами, підприємствами, установами, організаціями та посадовими особами, які сприяють виконанню покладених на неї завдань, а також громадянами України та їх об'єднаннями, іншими особами, які сприяють законній діяльності СБ України на добровільних засадах [5, ст. 8]. Закон України “Про основні засади забезпечення кібербезпеки України” деталізує сприяння Службі безпеки України як суб'єкту національної системи кібербезпеки: державні органи та органи місцевого самоврядування, їх посадові особи, підприємства, установи та організації незалежно від форми власності, особи, громадяни та об'єднання громадян зобов'язані сприяти суб'єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об'єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [1].

Закон України “Про телекомунікації” також передбачає підстави для взаємодії СБ України з операторами і провайдерами телекомунікацій, закріплюючи обов'язок останніх за власні кошти встановлювати на своїх телекомунікаційних мережах технічні

засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти проведенню оперативно-розшукових заходів та недопущенню розголошення організаційних і тактичних прийомів їх проведення; оператори телекомунікацій зобов'язані також забезпечувати захист зазначених технічних засобів від несанкціонованого доступу [6].

Частково питання взаємодії суб'єктів національної системи кібербезпеки передбачені у Правилах надання та отримання телекомунікаційних послуг, наприклад стосовно обов'язків споживачів: не допускати дій, що можуть перешкоджати безпечній експлуатації телекомунікаційних мереж, підтримці цілісності та взаємодії таких мереж, захисту їх інформаційної безпеки, електромагнітної сумісності радіоелектронних засобів, ускладнювати чи унеможлиблювати надання послуг іншим споживачам; не здійснювати несанкціонованого втручання в роботу та/або використання телекомунікаційних мереж [7], а також у Порядку підключення до глобальних мереж передачі даних [8], Правилах забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [9].

Безпосередньо правові підстави для взаємодії суб'єктів сектору безпеки і оборони, зокрема щодо захисту державних електронних інформаційних ресурсів (далі – ДЕІР), визначає Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах [10]. Зокрема, органи виконавчої влади з метою захисту державних інформаційних ресурсів в ІТС:

визначають перелік інформаційних та телекомунікаційних систем, які містять ДЕІР (у тексті документа використовується термін “державні інформаційні ресурси”, скорочення авторів), та погоджують його з Адміністрацією Держспецзв'язку (далі – Адміністрація);

здійснюють згідно з вимогами нормативно-правових актів з питань захисту інформації під методичним керівництвом Адміністрації заходи щодо захисту ДЕІР в інформаційно-телекомунікаційних системах (далі – ІТС), у тому числі підключених до глобальних мереж передачі даних;

збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків;

невідкладно (протягом доби) інформують Адміністрацію про спробу вчинення чи вчинення несанкціонованих дій;

надають на запит Адміністрації інформацію про технічні та програмні засоби, що використовуються для надання мережних послуг, а також про зміни у способах або видах підключення до глобальних мереж передачі даних;

оновлюють за рекомендаціями Адміністрації антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли державну експертизу.

У свою чергу Адміністрація: здійснює методичне керівництво та координує діяльність органів виконавчої влади, пов'язану із запобіганням, виявленням, реагуванням та усуненням наслідків несанкціонованих дій щодо ДЕІР в ІТС, надає в разі потреби допомогу у здійсненні заходів щодо запобігання порушенню цілісності, доступності та конфіденційності зазначених ресурсів; надає органам виконавчої влади відомості про антивірусні програмні засоби, які можуть застосовуватися для захисту ДЕІР в ІТС, та проводить перевірку їх оновлення; накопичує та аналізує дані про вчинення та/або спроби вчинення несанкціонованих дій щодо ДЕІР в ІТС, а також про їх наслідки, інформує правоохоронні органи для вжиття заходів із запобігання та

припинення злочинів у зазначеній сфері, оцінює стан захищеності цих ресурсів та надає відповідні рекомендації [10].

З метою організації координації діяльності з питань запобігання вчиненню порушень безпеки інформації в ІТС, виявлення та усунення наслідків інших несанкціонованих дій щодо ДЕІР в ІТС, а також впровадження єдиної процедури надання суб'єктами координації інформації про вчинення та/або спроби вчинення несанкціонованих дій щодо ДЕІР в ІТС розроблено Порядок координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо ДЕІР в ІТС [11]. Відповідно до цього Порядку суб'єкти координації у разі виявлення спроби вчинення та/або вчинення несанкціонованих дій вживають заходів щодо: блокування, усунення або локалізації їх негативних наслідків власними силами відповідно до Закону України "Про захист інформації в інформаційно-телекомунікаційних системах" та інших нормативно-правових актів у сфері ТЗІ; збереження (фіксації) ознак несанкціонованих дій, у тому числі на матеріальних носіях інформації; захисту ДЕІР відповідно до рекомендацій, наданих адміністратору безпеки ІТС електронною поштою, телефоном, факсом чи іншим способом; надсилання до Адміністрації Держспецзв'язку України письмового повідомлення тощо. Адміністрація Держспецзв'язку при цьому взаємодіє з органами державної влади, провайдерами та операторами телекомунікацій, установами, підприємствами та організаціями усіх форм власності України; для організації своєчасного обміну інформацією про несанкціоновані дії використовує веб-сторінку www.cert.gov.ua і електронні поштові адреси cert@cert.gov.ua та cert@dsszzi.gov.ua; здійснює міжнародне співробітництво з питань, що належать до компетенції Держспецзв'язку; з метою своєчасного запобігання та припинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж вживає заходів щодо своєчасного інформування правоохоронних органів України, зокрема і СБ України (додано Авт.) про виявлені суб'єктами координації несанкціоновані дії [11].

Правові та організаційні засади проведення оцінки стану захищеності ДЕІР в ІТС державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності визначені Порядком оцінки стану захищеності ДЕІР в ІТС [12]. Порядком визначається, що оцінка стану захищеності здійснюється з метою виявлення існуючих загроз ДЕІР в ІТС і є складовою частиною заходів із захисту інформації. Об'єктом оцінки стану захищеності є ДЕІР, які обробляються в ІТС, незалежно від наявності в таких ІТС комплексної системи захисту інформації (далі – КСЗІ). В ІТС, де створено КСЗІ з підтвердженою відповідністю, оцінка стану захищеності здійснюється з метою виявлення нових загроз ДЕІР, які виникли у процесі експлуатації КСЗІ та які не враховані у КСЗІ.

У разі виявлення в ІТС, де створено КСЗІ з підтвердженою відповідністю, додаткових загроз державним інформаційним ресурсам, які виникли за період експлуатації КСЗІ, інформація про таку КСЗІ надається Держспецзв'язку згідно з Положенням про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління, затвердженим постановою Кабінету Міністрів України від 03 серпня 2005 року № 688 [13]. У цьому напрямку правового регулювання нормативно-правові акти містять застарілі конструкції, відповідні

відносини потребують правового регулювання з урахуванням міжнародної практики, зокрема у частині запровадження аудиту інформаційної безпеки, про що йдеться нижче.

З метою здійснення оцінки стану захищеності Держспецзв'язку: створює комісію з оцінки стану захищеності (далі – комісія); здійснює планування проведення оцінки стану захищеності в державних органах, органах місцевого самоврядування, військових формуваннях, на підприємствах, в установах і організаціях незалежно від форм власності; визначає перелік документів, що стосуються функціонування ІТС та підлягають аналізу під час проведення оцінки стану захищеності; визначає та оприлюднює на офіційному веб-сайті Держспецзв'язку у мережі Інтернет перелік спеціалізованого ПЗ та програмно-апаратних засобів, які використовуються для проведення оцінки захищеності тощо. Державні органи, органи місцевого самоврядування, військові формування, підприємства, установи і організації незалежно від форм власності, в яких здійснюється оцінка стану захищеності: надають комісії всі необхідні документи, що стосуються функціонування ІТС; надають комісії доступ до ІТС; повідомляють Держспецзв'язку про стан виконання рекомендацій, зазначених в Акті [12]. При здійсненні таких перевірок (насамперед, позапланових) особливо важлива взаємодія Держспецзв'язку і СБУ. Адже наявні в обох органах на сьогодні технологічні можливості щодо виявлення кібератак та кіберінцидентів дають змогу спільно виявляти вразливості тієї або іншої ІТС, що обробляє ДЕІР.

Одним із механізмів посягань на ДЕІР є втручання в роботу офіційних веб-ресурсів органів державної влади. На сьогодні правові та організаційні засади проведення сканування на предмет вразливості ДЕІР, розміщених в Інтернеті, встановлює відповідний Порядок, який таке сканування передбачає як форму проведення оцінки стану захищеності інформації в ІТС. Сканування полягає у дистанційному виявленні уразливих місць програмно-апаратних засобів (місць, використовуючи які зловмисник може порушити цілісність, доступність, конфіденційність інформації або спостережність системи), які забезпечують функціонування ДЕІР, розміщених в Інтернеті. Об'єктом сканування є ІТС або її окремі елементи, в яких обробляються ДЕІР, розміщені в Інтернеті, незалежно від наявності в таких ІТС побудованої КСЗІ. До зазначених інформаційних ресурсів, зокрема, належать Інтернет-ресурси органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій державної форми власності.

До початку сканування підрозділ Держспецзв'язку: розробляє загальну програму та методику сканування; письмово погоджує із розпорядником ДЕІР, розміщеного в Інтернеті, та власником ІТС (якщо розпорядник ДЕІР не є власником ІТС, у якій обробляється відповідний ресурс) строки, обсяг та зміст проведення сканування; не пізніше ніж за три робочих дні письмово інформує Службу безпеки України про об'єкт, строки та методи проведення сканування. Передбачається також термінове інформування за допомогою електронної пошти. Крім того, Держспецзв'язку протягом п'яти календарних днів з моменту виявлення під час сканування випадків порушення правил обробки та захисту інформації, які можуть спричинити розголошення службової інформації або інформації, що становить державну таємницю, інформує про них Службу безпеки України [14].

Посадовим особам Держспецзв'язку, що безпосередньо проводять сканування, а також співробітникам Служби безпеки України, яким відповідно до визначених законодавством повноважень стали відомі результати сканування, забороняється використовувати виявлені вразливості для одержання доступу до змісту інформації, зокрема персональних даних, а також розголошувати результати сканування [14]. Цією

нормою встановлюються важливі правові гарантії захищеності відповідної інформації з обмеженим доступом.

Наведені вище приклади взаємодії між двома суб'єктами національної системи кібербезпеки передбачені адміністративними процедурами у сфері ТЗІ та перевірки відповідності захисту ДЕІР в ІТС, а також розміщеного в Інтернеті контенту, встановленим нормативним вимогам.

Відзначимо також, що Загальні вимоги до кіберзахисту об'єктів критичної інфраструктури (далі – Загальні вимоги), затверджені 19 червня 2019 р., вперше на загальнодержавному рівні (не враховуючи Постанову Правління Національного банку України від 28.09.2017 № 95 “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” [16]) визначають організаційно-методологічні, технічні та технологічні умови кіберзахисту об'єктів критичної інфраструктури. Відповідно до Загальних вимог власник та/або керівник об'єкта критичної інфраструктури організовує невідкладне інформування урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA (у разі наявності – галузевої команди реагування на комп'ютерні надзвичайні події), а також функціонального підрозділу ДКІБ СБУ (Ситуаційний центр забезпечення кібербезпеки СБУ) або відповідного підрозділу регіонального органу СБУ про кіберінциденти та кібератаки, які стосуються його об'єктів критичної інформаційної інфраструктури [16].

Новелою Загальних вимог є використання державними органами основного та резервного захищеного дата-центру збереження ДЕІР Державного центру кіберзахисту з метою створення резервних копій своїх інформаційних ресурсів та їх оперативного відновлення у разі пошкодження або знищення [16]. З урахуванням чисельних кібератак та кіберінцидентів, що виявляються як Держспецзв'язку, так і СБУ створення резервних копій ДЕІР є важливою передумовою збереження їх доступності і цілісності.

Зазначені вище нормативно-правові акти не враховують вимоги Закону України “Про основні засади забезпечення кібербезпеки України” у частині запровадження аудиту інформаційної безпеки. Тому у контексті розвитку державно-приватного партнерства підтримуємо необхідність врегулювання на рівні постанови Кабінету Міністрів України саме проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, проект якої було оприлюднено у квітні 2020 року [17]. Позитивним вважаємо включення до проекту регуляторного акта як вимог щодо проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури, так і порядку проведення такого незалежного аудиту.

Висловлюємо припущення, що зазначений правовий механізм (Загальні вимоги і незалежний аудит) має небагато шансів на успішне функціонування у межах держави без належного визначення переліку об'єктів критичної інфраструктури. А тому актуалізуємо необхідність прийняття такого акта. Позитивно відзначаємо, що на момент завершення цього дослідження, а саме 25 травня 2020 року Держспецзв'язку оприлюднив проект постанови Кабінету Міністрів України “Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури” [18]. Заслуговують на підтримку сформовані з урахуванням зарубіжного досвіду відповідної діяльності перелік секторів (підсекторів), основних послуг критичної інфраструктури, а також методика категоризації об'єктів критичної інфраструктури.

Насамкінець зазначимо, що проект закону про внесення змін до Закону України “Про Службу безпеки України” щодо удосконалення організаційно-правових засад діяльності Служби безпеки України [19] частково коригує статус СБУ як суб'єкта національної системи кібербезпеки. Хоча, на нашу думку, потребує термінологічних

правок. Зокрема, у зазначеному проекті закону використана редакція із Закону України “Про національну безпеку України”, який визначив СБ України державним органом спеціального призначення з правоохоронними функціями, що забезпечує державну безпеку, здійснюючи з неухильним дотриманням прав і свобод людини і громадянина:

- 1) протидію розвідувально-підбивній діяльності проти України;
- 2) боротьбу з тероризмом;
- 3) контррозвідувальний захист... кібербезпеки... та інформаційної безпеки держави, об’єктів критичної інфраструктури [20, ст. 31].

Однак, словосполучення “контррозвідувальний захист кібербезпеки” при визначенні відповідної функції СБ України видається не зовсім коректним. Вважаємо, що кращим для використання і позначення функції СБ України буде термін “контррозвідувальне забезпечення кібербезпеки”. Адже поняття “захист кібербезпеки” є етимологічно і змістовно не правильним.

Висновки.

Підсумовуючи викладене, зазначимо, що здійснений аналіз дав підстави для висновку про необхідність врегулювання окремих відносин, пов’язаних з розвитком національної системи кібербезпеки, з урахуванням міжнародної практики.

Зокрема, підтримано необхідність врегулювання на рівні постанов Кабінету Міністрів України:

процедури віднесення до об’єктів критичної інфраструктури з визначенням секторів (підсекторів) і методики категоризації об’єктів критичної інфраструктури;

незалежного аудиту інформаційної безпеки на об’єктах критичної інфраструктури.

З визначенням процедури віднесення до об’єктів критичної інфраструктури має запрацювати цілісний правовий механізм як кіберзахисту, що здійснюється Держспецзв’язку, так і контррозвідувального забезпечення СБУ кібербезпеки об’єктів критичної інформаційної інфраструктури.

Акцентовано також увагу на важливості взаємодії Держспецзв’язку і СБУ, зокрема при здійсненні перевірок суб’єктів, що оперують ІТС, в яких обробляються ДЕІР, з урахуванням наявних в обох органах технологічних можливостей щодо виявлення кібератак та кіберінцидентів.

Перспективами подальших наукових пошуків визначаємо питання правових механізмів для врегулювання питань державно-приватного партнерства у сфері кібербезпеки в Україні.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Hare, FB. Precision cyber weapon systems: An important component of a responsible national security strategy? *Contemporary security policy*. Т. 40. Вип. 2. С. 193-213. DOI: 10.1080/13523260.2018.1529369.
3. Patrascu, P. The Appearance and Development of National Cyber Security Strategies. *Proceedings Paper: 14th International Scientific Conference on eLearning and Software for Education - eLearning Challenges and New Horizons*. 2018. Vol 4. Стр. 53-59. DOI: 10.12753/2066-026X-18-222.
4. Stitilis, D, Pakutinskas, P, Malinauskaite, I. EU and NATO cybersecurity strategies and national cyber security strategies: a comparative analysis. *Security Journal*. 2017. № 30. С. 1151-1168.
5. Про Службу безпеки України: Закон України від 25.03.92 р. *Відомості Верховної Ради України*. 1992. № 27. Ст. 382.
6. Про телекомунікації: Закон України. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155. Ст. 39.

7. Про затвердження Правил надання та отримання телекомунікаційних послуг: Постанова Кабінету Міністрів України від 11.04.12 р. № 295. *Офіційний вісник України*. 2012. № 29. Ст. 1074, п. 36.

8. Про затвердження Порядку підключення до глобальних мереж передачі даних: Постанова Кабінету Міністрів України від 12.04.02 р. № 522. *Офіційний вісник України*. 2002. № 16. Ст. 864.

9. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.06 р. № 373. *Офіційний вісник України*. 2006. № 13. Ст. 878.

10. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах: Постанова Кабінету Міністрів України від 16.11.02 р. № 1772. *Офіційний вісник України*. 2002. № 47. Ст. 2155.

11. Про затвердження Порядку координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності з питань запобігання, виявлення та усунення наслідків несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Наказ Адміністрації Держспецзв'язку від 10.06.08 р. № 94. *Офіційний вісник України*. 2008. № 52. Ст. 1753.

12. Про затвердження Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Наказ Адміністрації Держспецзв'язку від 02.12.14 р. № 660. *Офіційний вісник України*. 2015. № 12. Ст. 323.

13. Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління: Постанова Кабінету Міністрів України від 03.08.05 р. № 688. URL: <https://zakon.rada.gov.ua/laws/show/688-2005-%D0%BF>

14. Про затвердження Порядку сканування на предмет вразливості державних інформаційних ресурсів, розміщених в Інтернеті: Наказ Адміністрації Держспецзв'язку від 15.01.16 р. № 20. *Офіційний вісник України*. 2016. № 17. Ст. 695.

15. Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України: Постанова Правління Національного банку України від 28.09.17 р. № 95. *Офіційний вісник України*. 2017. № 84. Ст. 2575.

16. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури: Постанова Кабінету Міністрів України від 19.06.19 р. № 518. *Офіційний вісник України*. 2019. № 50. Ст. 1697, п. 50.

17. Деякі питання проведення незалежного аудиту інформаційної безпеки на об'єктах критичної інфраструктури: проект постанови Кабінету Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=320263&cat_id=38837

18. Про затвердження Порядку віднесення об'єктів до об'єктів критичної інфраструктури: проект постанови Кабінету Міністрів України. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=321031&cat_id=38837

19. Про внесення змін до Закону України “Про Службу безпеки України” щодо удосконалення організаційно-правових засад діяльності Служби безпеки України: проект закону. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=68347

20. Про національну безпеку України: Закон України від 21.06.18 р. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.

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

УДК 340+35.078.3

ДОВГАНЬ О.Д., доктор юридичних наук, професор,  
НДІ інформатики і права НАПрН України  
ТАРАСЮК А.В., кандидат юридичних наук,  
НДІ інформатики і права НАПрН України

## ПРОТИДІЯ ЗАГРОЗАМ КІБЕРБЕЗПЕЦІ ДЕРЖАВИ НА ГЛОБАЛЬНОМУ РІВНІ

**Анотація.** У статті проаналізовано основні тенденції розвитку кіберпростору, а також визначені пов'язані із цим актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях, зокрема, у контексті забезпечення безпеки об'єктів критичної інфраструктури, становлення Інтернету речей тощо. За результатами дослідження визначені можливі шляхи вирішення відповідних проблем та підвищення ефективності забезпечення кібербезпеки.

**Ключові слова:** кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, кіберсистема, критична інфраструктура, інтернет речей.

**Summary:** The article analyzes the main trends in the development of cyberspace and identifies related cyber security issues at the global and national levels, in particular in the context of ensuring the security of critical infrastructure, the emergence of the Internet of Things and so on. According to the results of the study, the possible ways of solving the corresponding problems and improving the efficiency of providing cybersecurity were identified.

**Keywords:** cybersecurity, information security, cyberspace, cyber threats, cyber system, critical infrastructure, Internet of Things.

**Аннотация:** В статье проанализированы основные тенденции развития киберпространства, а также определены связанные с этим актуальные проблемы обеспечения кибербезопасности на глобальном и национальном уровнях, в частности, в контексте обеспечения безопасности объектов критической инфраструктуры, становление Интернета вещей и тому подобное. По результатам исследования определены возможные пути решения соответствующих проблем и повышения эффективности обеспечения кибербезопасности.

**Ключевые слова:** кибербезопасность, информационная безопасность, киберпространство, киберугрозы, киберсистемы, критическая инфраструктура, интернет вещей.

**Постановка проблеми.** Перші десятиліття 21 століття можна охарактеризувати як справжній прорив інформаційної греблі, коли хвилі інформаційних мереж і технологій досягли практично кожної людини. Глобальне поширення інформаційних мереж, передовсім Інтернету, зумовлює актуалізацію проблематики доступу до інформації, сумісності мереж тощо. Але водночас заходи із забезпечення безпеки глобальних мереж у теперішній важко визнати адекватними. Значною мірою це зумовлено тим, що загальносвітова соціально-економічна вагомість Інтернету виявилася дещо пізніше, а спочатку він замислювався як засіб якнайбільшого накопичення наукових даних і якнайшвидшого обміну ними. Відтак, відповідні безпекові заходи і засоби поки що змушені постійно наздоганяти стрімке поширення й удосконалення як конструктивних, так і зловмисних Інтернет-технологій.

Як і будь-яке досягнення науково-технічного прогресу, розвиток кіберпростору має як переваги, так і недоліки. До переваг може бути віднесені оперативність та розмаїття інформаційної взаємодії для ефективності розвитку всіх сфер людської діяльності,

розширення можливостей використання всього обсягу накопичених людством знань, тоді як до недоліків – розширення можливостей несанкціонованого доступу з будь-якої точки до будь-якої іншої точки кіберпростору, в тому числі й з протиправними намірами (саме такі можливості і розглядаються як загрози порушення нормального режиму функціонування кіберпростору, тобто, кіберзагрози). Динамічний розвиток світового кіберпростору істотно підвищує небезпеку реалізації кіберзагрози, актуалізуючи значну кількість проблем забезпечення кібербезпеки на глобальному та національному рівнях.

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

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

**Виклад основного матеріалу.** Сьогодні практично всі розвинені країни наразі розробили національні стратегії кібербезпеки, за якими здійснюватимуть захист своєї частини світового кіберпростору і участі в світовій кооперації вирішення виникаючих проблем. Розроблено та затверджено Міжнародний Стандарт ISO ІЕС 27032-2012 “Інформаційні технології – технології безпеки – вимоги для кібербезпеки”, відповідно до якого поняття “кібербезпека” розглядається як узагальнююче і включає в себе питання забезпечення безпеки систем, комунікацій і об’єктів, що входять до складу кіберпростору (інформаційної безпеки, безпеки мережевих структур, безпеки Інтернету, захисту критичної інформаційної інфраструктури тощо). До найважливіших положень Стандарту, на які мають орієнтуватися національні стратегії, слід віднести міжнародне співробітництво в реалізації спільних рішень, а також тісний контакт суспільства, держави і бізнесу в забезпеченні кібербезпеки.

Визначення актуальних питань протидії кіберзагрозам передбачає виділення критичних сфер національного кіберпростору, які вимагають захисту, і їх специфіки. До таких критичних сфер мають бути віднесені: інформаційна безпека, яку слід розглядати у широкому сенсі; безпека інформаційно-телекомунікаційного середовища, яка передбачає забезпечення безпеки всіх каналів і спеціальних систем зв’язку, що реалізують інформаційні взаємозв’язки будь-яких автоматизованих систем (систем органів державної влади, оборони, правопорядку, соціальної сфери, органів місцевого самоврядування, виробництва і технологічних процесів, корпоративних, громадських тощо) між собою і з зовнішнім світом; безпека автоматизованих систем управління і інформаційного забезпечення життєво важливих елементів національної інфраструктури.

У контексті загроз у кіберпросторі однією із основних проблем убачається здебільшого приватна належність інформаційно-комунікаційних мереж, тоді як на державу покладається значна частина відповідальності за їх безпеку. При цьому інтереси вказаних суб’єктів зазвичай різняться, що, звісно, не сприяє організації належного захисту інформаційної сфери з одночасним забезпеченням дотримання основних прав і свобод людини. Ситуація ускладнюється через глобальність як самої проблеми, так і методів і засобів її розв’язання.

На нашу думку, вагоме слово стосовно розробки міжнародно-правових норм щодо функціонування й захисту інформаційної сфери мають сказати міжнародні структури, створені для боротьби з кібернетичною злочинністю. З-поміж таких структур можна назвати, зокрема, підгрупу Великої вісімки з питань високотехнологічної (кібернетичної) злочинності, Конгрес ООН з питань профілактики злочинності та

кримінального судочинства, Конференція Ради Європи з питань співробітництва у сфері боротьби з кіберзлочинністю та ін. Вони здатні виступити координаторами оптимізації національних законодавств у частині регулювання питань притягнення до відповідальності (у тому числі кримінальної) за правопорушення у даній сфері, ведення слідчих дій та інших процесуальних моментів, гарантування недоторканності приватного життя та збереження особистих даних, забезпечення мережевої безпеки, адекватного реагування на кібератаки тощо. Убачається, що ці міжнародні структури можуть також посприяти виявленню прогалин у системі нагляду, формуванню дійових методів суспільного контролю над діяльністю суб'єктів боротьби з кібернетичними правопорушеннями.

Особливої уваги це питання потребує тому, що вказані міжнародні структури при розробці заходів протидії кіберзлочинності питання контролю відсувають на задній план, зосереджуючись переважно на дієвості. А тим часом, значні відмінності окремих національних законодавств, розрив у ресурсних і технічних потенціях різних країн ще більше актуалізують проблематику контролю й нагляду.

Приміром, величезні кошти у програми боротьби з кібернетичною злочинністю та вдосконалення відповідного законодавства вкладають уряди Великої Британії та США, тоді як чимало країн не мають не те що стратегій забезпечення кібербезпеки та боротьби з різновекторними кіберзагрозами, ба навіть базової інформаційної інфраструктури.

Брак технічних можливостей для ефективної боротьби з кібернетичними правопорушеннями, посилений слабким правовим забезпеченням, практично унеможлиблює їх розкриття і притягнення винних до відповідальності. Звідси випливає потреба розробки нормативно-правової бази сфери кібербезпеки й боротьби з кіберзлочинністю, зокрема й дійового регулювання питань суспільного контролю. Крім того, відсутність спеціальних державних наглядових інституцій підвищує загрози порушення прав людини на недоторканність приватного життя, свободу думки, об'єднань тощо.

Серед чинних міжнародно-правових документів у цій сфері слід назвати резолюції Генасамблеї ООН “Боротьба із використанням інформаційних технологій зі злочинною метою” від 4 грудня 2000 року 55/63 і від 19 грудня 2001 року № 56/121, а також ухвалені Всесвітньою конференцією “Співробітництво проти кіберзлочинності”, що відбулася 1 – 2 квітня 2008 року у Страсбурзі, “Головні принципи спільної роботи правоохоронних органів та Інтернет-провайдерів у сфері боротьби з кіберзлочинністю”. З-поміж відповідних регіональних правових актів варто виокремити Рекомендацію Ради Європи “Про боротьбу з комп'ютерними злочинами” (№ R(89)9) та Європейську Конвенцію “Про боротьбу з кіберзлочинністю”. Цей документ зобов'язує учасників Ради Європи передбачити в національних законодавствах повноваження відповідних органів, а також процедури для провадження розслідувань, зокрема для збирання електронних доказів у кримінальних злочинах, які вчинюються за допомогою комп'ютерних технологій.

Боротьби з кіберзлочинністю безпосередньо стосуються деякі правові акти щодо захисту прав людини міжнародного й регіонального характеру. Це, наприклад: ухвалений Генасамблеєю ООН у 1966 році Міжнародний пакт про громадянські й політичні права, де, зокрема, йдеться про права на недоторканність приватного життя (ст. 17), на свободу висловлення думки (ст. 19) та на свободу об'єднань (ст. 22); Європейська конвенція з прав людини, Американська конвенція з прав людини, Африканська хартія прав людини і народів та ін.

Захист електронних даних теж входить до функцій згаданих вище міжнародних і регіональних організацій. Так, положення щодо захисту прав на недоторканність приватного життя та свободу висловлення думки під час розміщення персональних даних в електронних мережах, електронного листування тощо містять ухвалені Генасамблеєю ООН “Принципи регулювання комп’ютеризованих баз персональних даних”, прийнята Радою Європи Конвенція “Про захист фізичних осіб у зв’язку з автоматизованою обробкою персональних даних” та ін.

Уряди багатьох країн в своїх стратегіях кібербезпеки приділяють особливу увагу інфраструктурі, тісно пов’язаної з питаннями безпеки. Для оцінки масштабу проблеми кібербезпеки і можливих загроз важливо розуміти взаємозв’язок між кібербезпекою й критичною інфраструктурою. Критична інфраструктура складається як з матеріальних (наприклад, будівель і споруд), так і віртуальних елементів (наприклад, систем і даних). Кожна країна може мати своє розуміння терміна “найважливіший”, проте зазвичай це поняття може включати в себе елементи інформаційно-комунікаційних технологій (включаючи електрозв’язок, енергетику, банківська справа, транспорт, суспільна охорона здоров’я, сільське господарство і продовольство, водопостачання, хімічну промисловість, судноплавство, а також найважливіші державні служби). Кожен з цих секторів економіки має свої власні матеріальні ресурси, наприклад будівлі банків, електростанції, поїзди, лікарні і урядові офіси. Разом з тим, всі ці найважливіші сектори національної економіки залежать від інформаційно-комунікаційних технологій. Відтак загальносвітові тенденції використання інформаційно-комунікаційних технологій роблять критичну інфраструктуру всіх секторів більш вразливою для кібератак.

Зокрема, актуальним для України є питання кіберзахисту цивільних ядерних об’єктів. Слід враховувати, що для цивільних ядерних об’єктів не існує універсальних стандартних рішень з інтеграції інформаційних технологій. Кожна атомна електростанція, її архітектури і топології є унікальним об’єктом, на якому реалізовані оригінальні рішення з такої інтеграції. Відповідно, в кожному випадку мереж та ІТ-системам такого об’єкта притаманний унікальний набір вразливостей кібербезпеки, що істотно обмежує можливості і практичний сенс застосування операторами цивільних ядерних об’єктів накопиченого досвіду і кращих іноземних практик. Існує проблема довіри до ІТ-постачальників і необхідність забезпечення цілісності ланцюжків поставок ІТ-продукції, більшість з яких – транснаціональні компанії. Відсутність конкурентоспроможних вітчизняних рішень на ринку змушує використовувати імпортні аналоги обладнання та програмного забезпечення. Таким чином, в даний момент ІТ-інфраструктура України (і це стосується не лише цивільних ядерних об’єктів) залежна від іноземних виробників і розробників, активно впроваджуючи їх вирішення (від бібліотек програмного забезпечення до апаратних платформ і систем управління). Фактично на кожній з ділянок ІТ-інфраструктури з високою часткою ймовірності використовуються закордонні рішення з невідомою “начинкою”. Рішенням цієї проблеми видається популярна в світі аутсорсингова модель виробництва, згідно з якою розробка і виведення на ринок затребуваних продуктів можливі лише за умови тісної кооперації з зарубіжними та вітчизняними компаніями. Це дозволяє на етапі проектування сформулювати концепцію нового продукту, пред’являючи йому затребувані ринком сучасні вимоги та передати стороннім спеціалізованим виробникам види робіт, які не є профільними для підприємства.

Системний підхід до питань кібербезпеки на рівні держави включає в себе не тільки підвищення обізнаності щодо існування ризиків в кіберпросторі, створення національних структур, що займаються питаннями кібербезпеки, а й встановлення



необхідних взаємин між різними групами учасників (держава, науково-дослідні інститути, розробники і виробники інфокомунікаційних рішень, замовники і споживачі), в тому числі між галузями економіки, для розвитку аутсорсингових моделі виробництва. Тож складність внутрішньої ІТ-інфраструктури і інтенсивність потоків даних на об'єктах критичної інфраструктури вимагають комплексного підходу до кібербезпеки, який принципово виходить за рамки тільки реагування на інциденти.

Слід зазначити кібератаки проти об'єктів критичної інфраструктури не підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинів і їх розслідування. Найбільш відомим механізмом такого роду є Будапештська конвенція про боротьбу з комп'ютерними злочинами, прийнята Радою Європи в 2001 році і відкрита для підписання всіма країнами. Схожа ситуація має місце щодо регіональних угод у сфері кібербезпеки, а також двосторонніх угод. Кіберінциденти на цивільних ядерних об'єктах та інших об'єктах критичної інфраструктури також не підпадають під дію юридично необов'язкових транскордонних механізмів співпраці, таких як альянс Міжнародного союзу електрозв'язку (МСЕ) і міжнародного державно-приватного партнерства ІМПАКТ або FIRST (міжнародний Форум взаємодії між центрами реагування на інциденти кібербезпеки). Крім того, наразі не вироблена міжнародна система стандартизації щодо специфічних ІТ-продуктів і сервісів, які поставляються операторам об'єктів критичної інфраструктури, відсутні загальні критерії і стандарти аудиту кібербезпеки на таких об'єктах.

Збільшення числа користувачів інтернету і розширення послуг онлайн послуг (за даними Gemius, станом на червень 2019 року в Україні число користувачів Інтернету становило 24,8 млн. осіб) призвело до зростання кіберзлочинності, в основному у фінансовій сфері. До найбільш істотних особливостей цього виду злочинів зазвичай відносять особливу складність їх розкриття та розслідування, надзвичайно високу їх латентність, прозорість національних кордонів для злочинців і відсутність єдиної правової бази для боротьби з ними, нерідко особливо великий розмір збитку, високопрофесійний склад осіб, які вчиняють такі злочини.

Сьогодні активно оцифровується сфера внутрішньої безпеки: документи, що засвідчують особу, камери відеоспостереження, електронні запити у кримінальних справах, перехоплення повідомлень стільникового зв'язку, системи моніторингу і збору інформації і тощо. Все це не тільки актуалізує проблему захисту персональних даних, а й уможливорює використання ІТ-комунікацій в організації громадських протестів або терористичних актів, а також управлінні можливими конфліктами. Саме тому суспільство потребує твердих гарантій її стійкості до кібератак та інших критичних ситуацій, незалежно від того, чи спрямовані такі атаки проти державних органів, комерційних підприємств або фізичних осіб.

Активне використання кіберпростору впливає і на людську особистість, зумовлюючи, окрім залежності від Інтернету, також і інші проблеми, зокрема, використання зловмисниками методів соціальної інженерії та вразливостей, пов'язаних з використанням Інтернету речей.

Можливості Інтернету речей (далі – IoT) дозволять віддалено керувати автомобілями, персональними медичними системами або змусити “розумний” холодильник здійснювати покупки, які не входили в плани власника. Мобільний банкінг дозволяє претворити будь-який гаджет в пристрій з функцією оплати. Однак, ототожнюючи фінансові відносини з ІТ-технологіями, не варто забувати і про поширення розкрадань грошових коштів, збоїв в роботі систем електронного банкінгу і, як наслідок, зростання операційних і репутаційних ризиків кредитно-фінансових організацій. Наразі

найбільший потенціал підвищення безпеки систем електронного банкінгу за допомогою ІТ вбачається у використанні біометричних даних (відбитки пальців або системи розпізнавання зовнішності) для посвідчення особи користувача.

Головна небезпека IoT полягає в тому, що ІТ-системи створюють нові точки доступу для зловмисників, які оперують у кіберпросторі – хакерів, кракерів тощо. Так, точкою входу до системи може стати мережевий принтер, який надає хакерам маршрут доступу до комп'ютерів в мережі фінансової організації, або мобільний пристрій, який має доступ до системи радіозв'язку високотехнологічного автомобілю тощо. При цьому кіберзлочинці йдуть завжди на крок попереду, вони нападають раптово і можуть використовувати нешаблонні способи атак, до яких не лише пересічні користувачі “розумної техніки”, але й служби безпеки та правоохоронці. У зв'язку із цим розробники та виробники засобів захисту змушені шукати нові рішення в умовах жорсткого ліміту часу, оскільки найбільша шкода виходить саме від так званих атак “нульового дня” (коли засобів протидії “інноваційним” атакам у кіберпросторі ще не винайдено). У деяких випадках захищатися взагалі доводиться від того, про що є вкрай поверхове уявлення: відсутні дані про кількість подібних атак, про способи, за допомогою яких безпосередньо здійснюється “вірусна інвазія” до програмного забезпечення, про алгоритмах дій зловмисників в певних ситуаціях тощо.

Ці та ряд інших важливих проблем кібербезпеки IoT слугували підставою випуску Технічним комітетом Європейського інституту телекомунікаційних стандартів (ETSI) з кібербезпеки стандарту кібербезпеки в Інтернет речей TS 103 645.

Документ встановлює базовий рівень безпеки для споживчих товарів, підключених до Інтернету, і закладає основу для майбутніх схем сертифікації IoT.

Згаданий стандарт, у частині захисту персональних даних, крім іншого, передбачає:

Положення 4.8-1. Виробники пристроїв і постачальники послуг зобов'язані надавати споживачам чітку і прозору інформацію про те, як, ким і з якою метою використовуються їхні персональні дані. Це також відноситься до третіх сторін, які можуть бути залучені, включаючи рекламодавців.

Положення 4.8-2. Якщо особисті дані обробляються на основі згоди споживачів, ця згода має бути отримана належним чином.

Положення 4.8-3. Споживачам, які дали згоду на обробку своїх персональних даних, повинна бути надана можливість відкликати згоду в будь-який час.

Минулого року Каліфорнія стала першим штатом США, де був прийнятий закон про кібербезпеку щодо IP-пристроїв (Закон № SB-327). Цей нормативно-правовий акт має набрати чинності у 2020 р.

У законі викладені вимоги до виробників пристроїв, які напряду чи опосередковано підключаються до Інтернету. Такі пристрої повинні передбачати “розумні” функції безпеки для запобігання несанкціонованого доступу, знищення, зміни чи крадіжки інформації. Положення закону спрямовані на захист звичайних користувачів. Законодавчі ініціативи щодо більш масштабних корпоративних рішень ще попереду.

Уряд Великобританії в минулому році випустив Звід практичних правил для забезпечення безпеки IP. В цьому нормативному акті акцент робиться на тому, що потрібно забезпечити кібербезпеку пристроїв, а не працювати над оновленням програмного забезпечення для посилення безпеки.

Значну увагу питанню кібербезпеки IP-пристроїв приділяє уряд Японії. В лютому 2019 р. японські чиновники з Національного інституту інформаційних та комунікаційних технологій оголосили про перевірку ефективності безпеки 200 млн.

IP-адрес у країні. Мета цього масштабного дослідження – виявити пристрої з низьким рівнем безпеки. Ця програма допоможе інтернет-провайдерам і телекомунікаційним компаніям краще зрозуміти вразливості в мережах та пристроях.

В ЄС Закон про кібербезпеку набрав чинності 27 червня 2019 р. Його положення закріплюють індивідуальні схеми сертифікації для певних категорій продуктів, процесів та послуг з IP-сфери. У сертифікатах має позначатися рівень гарантії безпеки та довіри до продукту, процесу чи послуги. Передбачається три рівні довіри. Найвищий відзначає успішне проходження всіх тестувань щодо кібербезпеки та повну гарантію для користувачів від виробника. Поки що застосування схем сертифікації не є обов'язковою вимогою для виробників IP-пристроїв. Це лише перші ініціативи, які намічають подальший напрямок законотворчості в цій сфері.

У даному контексті набуває загострення ще одна глобальна загроза – застосування штучного інтелекту виробниками зброї.

У звіті РАХ зазначено, щонайменше 30 світових виробників зброї займаються розробкою подібних систем озброєнь, і, як виявилось, вони роблять це набагато швидше, ніж політики домовляються про регулювання цього питання. У число розробників входять американські оборонні фірми Lockheed Martin, Boeing і Raytheon, китайські державні конгломерати AVIC і CASC, ізраїльські фірми IAI, Elbit і Rafael, Ростех Росії і турецька STM.

Більше занепокоєння у противників роботів-вбивць викликає розгортання штучного інтелекту в наступальних системах, які будуть вибирати і атакувати цілі самостійно, без людського контролю. Досі незрозуміло, як ця зброя буде відрізняти комбатантів від цивільного населення, або оцінювати пропорційність удару у відповідь. Юридичні експерти також не знають, хто буде нести відповідальність, якщо така автоматична зброя порушить міжнародне право. Без контролю людини ця зброя могла б полегшити розв'язання війни, зробивши її механічно жорстокою. В результаті застосування роботів-вбивць порушить основні правові та етичні принципи і дестабілізує міжнародний мир і безпеку, – зазначає автор звіту Рах Френк Слайпер.

Окрім зазначеного, особливо актуально знову постає проблема “іноземної залежності”. Як пересічні громадяни, так і оператори об'єктів критичної інфраструктури, державні органи та електронний уряд користуються іноземними операційними системами та антивірусними продуктами, що не сприяє забезпеченню кібербезпеки. В країні також використовується імпортне мережеве обладнання, яке може обслуговуватись зарубіжними розробниками дистанційно, а відтак – в “потрібний” момент виведено з ладу.

Крім того, існують і інші фундаментальні проблеми, що виникають внаслідок розвитку інформаційно-комунікаційних технологій та Інтернету речей. Так, психологи попереджають про загрози інтелектуальної деградації особистості через надмірно тривалого перебування в мережі, ігроманії, манії переслідування, страх втратити свій комунікатор, порушеннях пам'яті (здатності запам'ятовувати числа і факти), виснаження інтуїції, що в цілому може привести до ослаблення інтелектуального потенціалу людини. До того ж постійне використання зовнішніх пристроїв знижує рівень щастя (умовне значення міжнародного індексу щастя, Happy Planet Index) населення. Інтернет-залежність сприяє також на імплементацію населенню сторонніх культурних кодів, нав'язування вигідної іноземним державам світоглядної картини.

Відтак розвиток заходів щодо зміцнення кібербезпеки має здійснюватися на відмінній від інших держав базі, а в ідеалі слід формувати власну програмну платформу. Крім того, слід розробляти власні криптографічні програми. Зокрема, партнерські

відносини з вітчизняними розробниками ІТ-технологій, криптографічних засобів захисту тощо дають державі не лише безпосередньо технології, знання, фахівців, мале й оживість створення власних, контрольованих рішень. Відповідно, в усіх розвинених країнах існують компанії з розробки антивірусів та інших рішень у сфері кібербезпеки.

Цілком зрозуміло, що без участі пересічних користувачів мережі боротьба з кіберзлочинністю навряд чи буде достатньо ефективною. Відтак, убачається необхідним залучати їх до заходів із роз'яснення прав користувачів всесвітньої мережі Інтернет, етичних аспектів її функціонування, варіантів і механізмів комп'ютерних шахрайств, викрадення особистих реквізитів та інших Інтернет-злочинів.

Таблиця 2.1. Джерела кібернетичних загроз<sup>1</sup>

| Джерело загрози   | Зміст загрози                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Держава</b>    | <p>Спеціальні (розвідувальні) служби держави застосовують для збирання відкритої інформації та шпигунства стосовно інших держав (не тільки ворожих, а й союзних) або недержавних суб'єктів кібернетичних атак комп'ютерні технології.</p> <p>Проти ворожих держав (суб'єктів) з метою дезінформації, залякування, дестабілізації, аж до кібернетичної війни, можуть здійснюватися кібератаки.</p> <p>Можуть також здійснюватися перехоплення персональних даних та їх використання. Подеколи це відбувається без передбаченого законом санкціонування та належного демократичного контролю, що порушує права людини.</p> |
| <b>Корпорації</b> | <p>Приватні корпорації чи підприємства займаються промисловим шпигунством, диверсіями тощо, нерідко залучаючи для цього хакерів, організовані злочинні угруповання і т.п.).</p> <p>Як і в разі державних спецслужб, корпорації, збираючи, аналізуючи й використовуючи значні обсяги персональних даних, обмінюючись ними з іншими суб'єктами (як приватними, так і державними), можуть порушувати права людини.</p>                                                                                                                                                                                                      |
| <b>Хакери</b>     | <p>У теперішній час хакерство, яке розпочиналось зі зламування комп'ютерних мереж для професійного вихваляння або ж із хуліганською метою, все більше набуває кримінального характеру. Усе більш витонченими й доступними стають засоби для здійснення кібератак, інструкції щодо застосування яких не важко знайти в Інтернеті. Тому сьогодні для проникнення у віддалені мережі вже не треба, як раніше, глибокі знання й віртуозне володіння комп'ютерними технологіями.</p>                                                                                                                                          |
| <b>Хактивісти</b> | <p>Хактивізм (англ. <i>hack</i> – прорубуватися, проникати та <i>activism</i> – активність, діяльність) – соціальне явище, соціальних протестний рух за допомогою хакерства – незаконного проникнення у певні веб-сайти чи поштові сервери з метою їх пошкодження, викривлення, спотворення чи руйнації для досягнення певних політичних цілей.</p>                                                                                                                                                                                                                                                                      |

<sup>1</sup> За матеріалами United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity," *Science* 326 (13 November 2009): 943-4; см. Martin Charles Golumbic, *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).

|                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Кібер-диверсанти<br/>із числа<br/>невдоволених<br/>користувачів</b> | Цей контингент являє собою неабияку загрозу, позаяк це зазвичай люди, котрі непогано обізнані з принципами функціонування мережі й можуть скористатися цим для пошкодження системи, викрадення конфіденційної інформації чи з іншою протиправною метою. Як з'ясували фахівці ФБР США, ймовірність організації кібернетичних атак користувачами системи вдвічі вища ніж зовнішніми суб'єктами.                                                                                                                                                                                                                                                        |
| <b>Терористи</b>                                                       | З метою досягнення своєї мети терористи намагаються спричинити масові людські жертви, вивести з ладу чи знищити об'єкти критичної інфраструктури, створити загрози національній безпеці, дестабілізувати економіку, порушити моральний стан суспільства, підірвати авторитет державної влади тощо.<br>У теперішній час ті терористичні угруповання, які ще не мають технічних можливостей і фахівців для проведення кібератак, усе частіше звертаються до "послуг" організованих злочинних структур або ж намагаються отримати відповідні знання та фахівців, що сьогодні цілком реально.                                                            |
| <b>Ботнет</b>                                                          | Бот – програма у складі ботнету, яка приховано впроваджується у пристрій зловмисної зацікавленості й дає хакерів змогу, використовуючи ресурси комп'ютера жертви, провадити певні дії. Заражаючи такими програмами значну кількість пристроїв, хакери користаються ними для здійснення й координування кібератак, фішингу, перебору паролів на віддалених системах, розсилання спаму та інших шкідливих незаконних операцій. На рику нелегальної торгівлі широкий асортимент подібних "послуг" користується неабияким попитом.                                                                                                                       |
| <b>Фішери</b>                                                          | Фішинг (англ. <i>phishing</i> – виуджування) – незаконний спосіб отримання персональної інформації – паролів, номерів банківських рахунків чи кредитних карт тощо шляхом розсилання від імені банку електронних листів з посиланнями на підроблені сайти, які імітують роботу справжніх, або створення точної копії існуючої банківської веб-сторінки, аби змусити користувача ввести свої особисті фінансові дані; використовуються також шпигунські та інші шкідливі програми, спами).<br>Фішери – окремі особи чи групи, котрі використовують вказаний вид інтернет-шахрайства у власних протиправних цілях чи з метою перепродажу добутих даних. |
| <b>Спамери</b>                                                         | Спамери – це фізичні чи юридичні особи, котрі з метою реклами займаються розповсюдженням незатребуваної електронної пошти – спаму, який нерідко містить недостовірну або приховану інформацію. Розсиланням спаму може також приховуватися фішинг, поширення шпигунського чи шкідливого програмного забезпечення, кібератаки тощо.                                                                                                                                                                                                                                                                                                                    |
| <b>Виробники<br/>шпигунського чи<br/>шкідливого ПЗ</b>                 | До цієї категорії належать фізичні чи юридичні особи, котрі виробляють шпигунське чи шкідливе програмне забезпечення і шляхом його розповсюдження здійснюють кібератаки.                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Педофіли</b>                                                        | Можливості всесвітньої мережі – електронна пошта, спеціалізовані файлообмінні сервіси, пірінгове програмне забезпечення, соціальні мережі, чати тощо – все частіше використовується педофілами з метою обміну дитячою порнографією та задля пошуку потенційних жертв і знайомства з ними.                                                                                                                                                                                                                                                                                                                                                            |

Таблиця 2.2. Види кібернетичних загроз

| Вид загрози                                                                                                                                                                                                           | Підвид загрози                | Зміст та приклади                                                                                                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Цілісність даних</b><br>Для викривлення, спотворення, знищення даних чи порушення їхньої цілісності в інший спосіб можуть застосовуватися хакерські методики.                                                      | Пропаганда, дезінформація     | Зміна (викривлення) даних чи впровадження хибних даних для впливу на суспільно-політичні процеси, результати економічної, бізнесової діяльності або ж з метою дестабілізації обстановки (правлячих режимів) в іноземній країні.                                    |
|                                                                                                                                                                                                                       | Залякування                   | Кібератаки здійснюються з метою примусити приватних чи державних власників веб-сайтів змінити (видалити) їх зміст або ж усю політику ресурсу.                                                                                                                      |
|                                                                                                                                                                                                                       | Знищення                      | Систематичне цілеспрямоване нищення певних даних іноземної держави чи конкурента. Зазвичай здійснюється в комплексі з іншими підливними заходами у процесі відповідних операцій.                                                                                   |
| <b>Доступ</b><br>Створення умов, коли законні (легітимні) користувачі не в змозі отримати доступ (або цей доступ ускладнений) до певних серверів (ресурсів), що їх надає система (атаки на відмову в обслуговуванні). | Зовнішня інформація           | Подібні й інші атаки на державні та приватні ресурси відкритого доступу (інформаційні сайти державних структур, ЗМІ та ін.).                                                                                                                                       |
|                                                                                                                                                                                                                       | Внутрішня інформація          | Кібератаки на локальні мережі державних чи приватних структур – управління об'єктами критичної інфраструктури, транспорту, аварійно-рятувальних служб, кредитно-банківських установ, системи оперативного управління, корпоративні сервіси електронної пошти тощо. |
| <b>Конфіденційність</b><br>Кібернетичні атаки зі злочинним умислом спрямовані на різноманітні джерела (ресурси) конфіденційної інформації.                                                                            | Шпигунство                    | Шпигунська діяльність держав щодо іноземних держав, фізичних та юридичних осіб; здобуття конкурентними суб'єктами інформації про своїх опонентів.                                                                                                                  |
|                                                                                                                                                                                                                       | Викрадення персональних даних | Фішинг та подібні кібератаки з метою у шахрайський спосіб з'ясувати персональні дані користувачів, зокрема номери їхніх банківських рахунків, а також упровадження вірусів для зняття даних з комп'ютера жертви тощо                                               |

|  |                                                           |                                                                                                                                                                                                                                                                              |
|--|-----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | “Крадіжка особистості”<br>(викрадення персональних даних) | З метою викрадення персональних даних особи та використання їх для вчинення протизаконних дій застосовуються вірусні троянські й аналогічні програми                                                                                                                         |
|  | Пошук інформації в Інтернеті                              | Технології пошуку інформації з відкритих джерел застосовуються з метою здобуття різноманітної інформації, зокрема персональних даних.                                                                                                                                        |
|  | Шахрайство                                                | Цей злочин нерідко вчинюється за допомогою спаму, який розповсюджується через електронну пошту. Славнозвісними у цьому сенсі стали так звані “нігерійські листи 419”. З-поміж поширених подібних шахрайських схем – пропозиції щодо передоплати фіктивних товарів чи послуг. |

Шкідливі дії в кіберпросторі з погляду порушення властивостей інформації та інформаційних мереж вчиняються з метою:

- порушення конфіденційності шляхом несанкціонованого доступу до наявних в інформаційній системі даних;
- порушення цілісності шляхом несанкціонованих змін чи модифікації інформаційних систем і даних, що в них зберігаються;
- порушення доступності шляхом зловмисного перешкоджання доступу до інформаційних систем і даних, що в них зберігаються.

За походженням можна виокремити природні й антропогенні (рукотворні) загрози. До перших належать загрози, пов’язані з явищами природи, стихійними катаклізмами – буревії, повені, пожежі, землетруси, цунамі тощо, а також загрози техногенні, пов’язані з технічними проблемами. Натомість антропогенні загрози впливають із дій людини стосовно інформації, комп’ютерних систем і мереж. Вони поділяються на неумисні й умисні. З-поміж останніх загроз можна виокремити адресні атаки, ціллю яких є певна інформаційна система або ж об’єкт критичної інфраструктури, а також безадресні атаки, котрі не мають конкретної цілі (приміром, розповсюдження шкідливих програм).

Слід зауважити, що саме рукотворні загрози є головними викликами інформаційній безпеці, про що свідчить зростання й урізноманітнення методів і засобів зловмисних дій у кібернетичному просторі. Джерелом таких дій і відповідних загроз стають численні суб’єкти, котрі мають достатні знання й можливості для вчинення шкідливих дій в інформаційному середовищі.

Серед основних суб’єктів (джерел) кіберзагроз можна виокремити такі:

- держави, які використовують відповідні кіберзасоби для збирання інформації та розвідувальної діяльності (зокрема, економічне шпигунство задля отримання переваг в економічній, політичній, військовій та інших сферах); деякі держави вдаються до засобів інформаційної війни з метою обмеження противної сторони у прийнятті рішень, отримання стратегічних і тактичних переваг, руйнації окремих об’єктів (критичної інфраструктури, в тому числі пов’язаних з оборонною сферою);

- бізнесові структури: приватні компанії-конкуренти, котрі прагнуть здобути важливі дані щодо опонентів задля отримання ринкових переваг – виробництво, ціни, розробки, асортимент тощо;

- кримінальні угруповання, котрі вдаються до кібернетичних атак з метою грошового зиску; засоби, що при цьому застосовуються, найрізноманітніші: фішинг, спам, шкідливі програми для Інтернет-крадіжок, комп'ютерного вимагання, викрадення персональних даних тощо;

- міжнародне корпоративне шпигунство, метою якого є економічне, промислове шпигунство, викрадення значних коштів; нерідко користуються послугами хакерів, надаючи їм відповідні засоби;

- мережеві оператори, котрі використовують ботнет (мережу) дистанційно керованих зламаних систем задля розповсюдження спаму, фішингу, провадження узгоджених атак та ін.;

- розробники шкідливих програм і програм стеження – окремі особи чи організації, котрі створюють і застосовують вказаний продукт з протиправною метою;

- розробники фішингових схем, котрі створюють і застосовують їх для викрадення коштів, персональних даних тощо;

- працівники підприємств (компаній, установ), які мають доступ до внутрішньої конфіденційної інформації (інсайдери), у тому числі до комп'ютерних систем, а тому можуть викрадати дані або завдавати шкоди. До цих суб'єктів належать також некваліфіковані чи халатні співробітники, тимчасово наймані працівники, котрі можуть неумисно зашкодити системі через необережність;

- спамери, котрі використовують схеми фішингу, поширюють у мережі повідомлення, які містять приховані або хибні дані, а також шпигунські й вірусні програми, здійснюють кібератаки (приміром, "відмова в обслуговуванні" – DDoS);

- терористи, котрі ставлять за мету виведення з ладу чи руйнацію об'єктів критичної інфраструктури або ж втручання у їх функціонування, що може призвести до значних людських жертв, становить серйозну загрозу національній безпеці через підрив економіки країни, морально-психологічного стану суспільства. Ця категорія для отримання грошового зиску та важливої інформації також вдається до шпигунських та інших шкідливих програм, фішингу та ін.;

- хакери, котрі зламують закриті інформаційні системи й мережі з різних мотивів. Це може бути перевірка фахових здібностей, самоствердження, демонстрація певної громадянської позиції, отримання незаконного фінансового зиску;

- хактивісти, котрі з метою розміщення матеріалів політичного характеру атакують поштові сервери та веб-сторінки.

Усе наведене вище переконливо свідчить, що для забезпечення інформаційної безпеки необхідні здійснення комплексу заходів, скоординовані зусилля державних органів, бізнесових структур та окремих громадян. Особливо це стосується злагодженої взаємодії державного й приватного секторів, позаяк в останньому перебуває значна частина мереж і критичної інфраструктури. Відтак, неабиякого значення набуває підвищення загальної відповідальності за безпекову сферу, налагодження дійової міждержавної взаємодії та ефективного зворотного зв'язку.

### **Висновки.**

В цілому розвиток інформаційних технологій – процес з потужним потенціалом та надприбутковий бізнес. Наприклад, в Кореї обсяг системи E-learning (навчання за допомогою Інтернет і мультимедіа) щорічно зростає на 8,2 %, і вже працює близько 20 віртуальних університетів. Разом з тим, існує дуже мало систематизованої інформації



про безпеку в кіберпросторі, поданої в доступній формі. В Україні також існує гостра необхідність запуску програми навчання населення. Вона повинна бути розрахована не тільки на вузькоспеціалізовані структури, а й на вивчення основ кібербезпеки в школах і інститутах, а також навчання людей, що вийшли з шкільного та студентського віку. Для інформування та навчання необхідно, в тому числі, створити інформаційно-консультаційний центр, де користувачі зможуть отримувати відповіді на питання, пов'язані з кіберзагрозами і кіберзахистом. Одним з перших кроків в цьому напрямку може вважатися, наприклад, створення у 2017 році інформаційної площадки (Antivirus.ua), місією якої є створення умов для обміну кваліфікованою інформацією між рядовими користувачами, експертами, представниками ЗМІ, навчальних закладів тощо.

Таким чином, швидка інформатизація, масштаби потенційних наслідків злочинів у кіберпросторі, недостатня кіберзахищеність об'єктів критичної інфраструктури та ризики, пов'язані з розвитком психологічної Інтернет-залежності вимагають від національних урядів та міжнародної спільноти серйозної уваги до розвитку систем кібербезпеки на національному та глобальному рівнях. Першочергові кроки в цьому напрямку повинні передбачати розробку необхідної нормативно-правової бази і підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду в цій сфері. Зокрема, перспективний підхід до забезпечення кібербезпеки об'єктів критичної інфраструктури має передбачати: забезпечення кібербезпеки на етапі проектування об'єктів критичної інфраструктури; виявлення мережевих подій, реагування на них, а також моніторинг мережевого трафіку в режимі реального часу для всіх ІТ-контурів об'єктів критичної інфраструктури; введення нових вимог до постачальників критично важливих ІТ-комплектуючих об'єктів критичної інфраструктури (наприклад, зобов'язання постачальника розкривати оператору цивільних ядерних об'єктів вихідний код прошивки програмних логічних контролерів після підписання контракту на постачання); впровадження рішень з криптографічного захисту інформації, а також цифрових підписів і захищених міток часу на всіх мережевих рівнях об'єктів критичної інфраструктури для більш надійного захисту цілісності та конфіденційності даних.

Розробка та впровадження рішень з криптографічного захисту інформації, так само, як і розробка васних операційних систем, мережевих платформ, комунікаторів тощо, на сучасному етапі є необхідними заходами для забезпечення кібербезпеки (як кібербезпеки об'єктів критичної інфраструктури та інших технічних об'єктів, так і інформаційно-психологічної безпеки людини у кіберпросторі) на національному рівні.

На глобальному рівні, зважаючи на те, що не всі кібератаки підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинам, для забезпечення кібербезпеки важливим є передбачити зобов'язання держав не вдаватися у кіберпросторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо, заради здійснення підризу політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави, відповідно до підходів, окреслених у Резолюції 60/45 Генеральної Асамблеї ООН "Досягнення в сфері інформатизації і телекомунікацій в контексті міжнародної безпеки".

### Використана література

1. ISO/IEC 27032:2012. Information technology – Security techniques – Guidelines for cybersecurity. URL: <https://www.iso.org/standard/44375.html>

2. Кибербезопасность гражданских ядерных объектов: оценка угрозы и пути ее преодоления. URL: <http://pircenter.org/media/content/files/13/14875347670.pdf>
3. Кибербезопасность объектов критической ядерной инфраструктуры. URL: <http://pircenter.org/projects/46-cybersecurity-of-critical-nuclear-infrastructure>
4. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України (аналітична доповідь). URL: [http://old2.niss.gov.ua/content/articles/files/AD\\_Dubov\\_206x301\\_pp1-84\\_press-b44d7.pdf](http://old2.niss.gov.ua/content/articles/files/AD_Dubov_206x301_pp1-84_press-b44d7.pdf)
5. Ревенков П.В. Финансовый мониторинг в условиях интернет-платежей. Москва: КноРус, 2016. С. 64-67.
6. Ревенков П.В., Бердюгин А.А. ДБО: Интернет создает новых клиентов и расширяет профили рисков. *Банковское дело*. 2013. № 12. С. 64-67.
7. CYBER; Cyber Security for Consumer Internet of Things. ETSI TS 103 645 V1.1.1 (2019-02). URL: [https://www.etsi.org/deliver/etsi\\_ts/103600\\_103699/103645/01.01.01\\_60/ts\\_103645v010101p.pdf](https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf)
8. Slippery Slope. PAX. URL: <https://www.paxforpeace.nl/publications/all-publications/slippery-slope>
9. Ткачук Т. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. *Підприємництво, господарство і право*. 2017. № 10. С. 182-186.
10. Скиннер К. Цифровой банк: как создать цифровой банк или стать им. Москва: Манн, Иванов и Фербер, 2015. 320 с.
11. Крупенникова Л.Ш., Курбатов В.И. Виртуальная личность: Net-мышление, сетевой психотип, и Интернет-фобии. URL: <https://cyberleninka.ru/article/n/virtualnaya-lichnost-net-myshlenie-setevoj-psihotip-i-internet-fobii/viewer>
12. Ситнова И.В., Поляков А.А. Информационно-психологическое воздействие как практика ведения войн четвертого поколения. URL: <https://cyberleninka.ru/article/n/informatsionno-psihologicheskoe-vozdeystvie-kak-praktika-vedeniya-voyn-chetvertogo-pokoleniya>
13. За матеріалами United States Government Accountability Office, Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk (Washington DC: US GAO, 2009); William A. Wulf and Anita K. Jones, "Reflections on Cybersecurity". *Science* 326 (13 November 2009): 943-4; см. Martin Charles Golumbic. *Fighting Terror Online: The Convergence of Security, Technology, and the Law* (New York: Springer, 2007).
14. Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain. United States Government Accountability Office. September 10, 2007. P. 12. URL: <http://www.gao.gov/assets/270/268137.pdf>
15. Wilshusen, Gregory C. Information Security: Cyber Threats and Vulnerabilities Place Federal Systems at Risk. Testimony Before the Subcommittee on Government Management, Organization, and Procurement; House Committee on Oversight and Government Reform United States Government Accountability Office. May 5, 2009. P. 3. URL: <http://www.gao.gov/assets/130/122454.pdf>
16. Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности: Резолюция 60/45, принятая Генеральной Ассамблеей Организации Объединенных Наций. URL: [https://zakon.rada.gov.ua/laws/show/995\\_e45](https://zakon.rada.gov.ua/laws/show/995_e45)

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

УДК 340.132.6:341.48

ХАХАНОВСЬКИЙ В.Г., доктор юридичних наук, професор, професор кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ.
ORCID: <https://orcid.org/0000-0001-5676-5641>.

ГАВЛОВСЬКИЙ В.Д., кандидат юридичних наук, с.н.с., головний науковий співробітник Міжвідомчого НДЦ з проблем боротьби з організованою злочинністю при РНБО України.

ТЛУМАЧЕННЯ ТА КЛАСИФІКАЦІЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ ЯК КІБЕРЗЛОЧИНІВ

Анотація. Розглянуто проблеми тлумачення та класифікації кіберзлочинів, проведено аналіз статистичної звітності Національної поліції України щодо показників про кіберзлочинність. Пропонується перелік “традиційних” кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів. Надаються рекомендації щодо кваліфікації окремих кіберзлочинів.

Ключові слова: кіберзлочин, класифікація кіберзлочинів, статистичні показники, “традиційні” кримінальні правопорушення як кіберзлочини.

Summary. The problems of interpretation and classification of cybercrimes are considered, the analysis of statistical reporting of the National Police of Ukraine on indicators of cybercrime is carried out. A list of “traditional” criminal offenses that may fall into the category of cybercrime is proposed. Recommendations on the qualification of individual cybercrimes are provided.

Keywords: cybercrime, classification of cybercrimes, statistical indicators, “traditional” criminal offenses as cybercrimes.

Аннотация. Рассмотрены проблемы толкования и классификации киберпреступлений, проведено анализ статистической отчетности Национальной полиции Украины относительно показателей о киберпреступности. Предлагается перечень “традиционных” уголовных правонарушений, которые могут относиться к категории киберпреступлений. Даются рекомендации в отношении квалификации отдельных киберпреступлений.

Ключевые слова: киберпреступление, классификация киберпреступлений, статистические показатели, “традиционные” уголовные правонарушения как киберпреступления.

Постановка проблеми. Злочинність, яка є невід’ємною частиною суспільства, існувала в усі часи, існує вона й у віртуальному просторі як кіберзлочинність. Водночас офіційного, закріпленого в міжнародних документах визначення кіберзлочинності поки не існує. Тим не менш це не заважає визначати діапазон спеціальних слідчих повноважень і можливостей в сфері міжнародного співробітництва, які більшою мірою стосуються виявлення електронних доказів вчинення будь-якого злочину, зокрема, в межах Конвенції Ради Європи про кіберзлочинність (далі – Конвенція).

Разом з тим, відносно кримінальних правопорушень, що становлять основу кіберзлочинності, деякі визначення необхідні. Зокрема, для розробки правових заходів боротьби з цим видом правопорушень на національному рівні, для збирання та аналізу статистичних даних, вироблення системи єдиного обліку на глобальному рівні тощо.

Крім того, для боротьби з кіберзлочинністю необхідно, в першу чергу, мати перелік суспільно небезпечних винних діянь у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну

відповідальність та/або яке визнано злочином міжнародними договорами України, тобто перелік злочинів, які можуть кваліфікуватися як кіберзлочини.

Варто зазначити, що термін “кіберзлочинність” часто вживається поряд з термінами “комп’ютерна злочинність”, “злочинність в сфері високих інформаційних технологій” тощо. Причому нерідко ці поняття використовуються як синоніми. Тобто доктринальні підходи до розуміння поняття кіберзлочин є різними. Проте попри наявні альтернативні дефініції саме термін кіберзлочинність найбільшою мірою відображає сутність зазначеного явища.

В національному законодавстві України – в Законі України “Про основні засади забезпечення кібербезпеки України” від 05.10.17 р. № 2163-VIII, кіберзлочинність визначається як сукупність кіберзлочинів. А кіберзлочин (комп’ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Результати аналізу наукових публікацій. Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як Н.М. Ахтирська, В.М. Бутузов, В.О. Голубев, М.В. Гуцалюк, С.В. Демедюк, В. Шеломенцев та ін. [2 – 7]. Проте у вітчизняному законодавстві не існує чіткого визначення поняття кіберзлочин. Дискутуються також різні точки зору щодо класифікації кіберзлочинів. У зв’язку з появою новітніх інформаційних технологій та способів вчинення кіберзлочинів, ці питання потребують подальшого дослідження та ретельного вивчення як науково-теоретичної проблеми.

Метою статті є визначення класифікацій кіберзлочинів, які надаються в офіційних документах, зокрема ООН, ЄС, та дослідженнях науковців, через які розкривається поняття кіберзлочинності, визначення переліку кримінальних правопорушень, які можуть відноситися до категорії кіберзлочинів та аналіз статистичної звітності Національної поліції України щодо показників про кіберзлочини.

Виклад основного матеріалу. Підхід щодо класифікацій кіберзлочинів, через які розкривається поняття кіберзлочинності, є досить загальним, але водночас відображає специфіку даного виду злочинів.

Насамперед, варто зазначити, що Конвенція про кіберзлочинність є єдиним зобов’язуючим міжнародним інструментом у сфері протидії кіберзлочинності. Вона містить набір основних принципів для будь-якої країни, що розробляє національне законодавство з протидії кіберзлочинності. Разом з тим, наведена в Конвенції класифікація, на думку низки західних і вітчизняних дослідників, не є всеосяжною. Спочатку в Конвенції кіберзлочини поділялися на чотири групи. Потім, на початку 2002 р. на додаток до Конвенції ухвалили протокол, який доповнив перелік злочинів поширенням інформації расистського й іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, релігійній або етнічній приналежності. Із розвитком науково-технічного потенціалу і громадських відносин у кіберпросторі згаданий список буде, на жаль, розширюватися. До того ж зазначені в Конвенції злочини пов’язані з деякими, але не з усіма діями, які посягають на громадську безпеку. Разом з тим, іншу думку висловлюють науковці, яким імпонує система кіберзлочинів, передбачена Конвенцією.

У звіті Комітету внутрішніх справ Парламенту Великобританії щодо кіберзлочинності у 2013 році кіберзлочини поділяють на три категорії:

– виключно мережеві злочини, де цифрові системи є основною ціллю, що одночасно виступають і засобами посягання. Ця категорія включає в себе посягання на

комп'ютерні системи для знищення інфраструктури інтернет-технологій та незаконне заволодіння даними;

- існуючі злочини, що були переведені в площину кіберзлочинів через використання Інтернету;

- використання Інтернету з метою торгівлі наркотиками та як допоміжний інструмент для вчинення інших видів злочинів [8].

У спільному повідомленні Європейської Комісії у 2013 р. до Європейського Парламенту, Ради, Європейського економіко-соціального комітету та Комітету регіонів кіберзлочинність також розкривається через три основні категорії:

- традиційні види злочинів (шахрайство, підробка документів і т.п.), що вчиняються з використанням електронних комунікаційних мереж та інформаційних систем;

- розміщення незаконного контенту в електронних медіа;

- атаки на інформаційні системи, блокування програмного забезпечення сайтів і хакерство [9].

Більшість дослідників, які вивчають проблему кіберзлочинності, пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета посягання. Найпоширеніший поділ як варіант – це комп'ютерні злочини та злочини, вчинені за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв для доступу до кіберпростору. Ця позиція підтримується і тим, що на Десятому Конгресі Організації Об'єднаних Націй з профілактики злочинності і поведження з правопорушниками, де розглядалися заходи щодо боротьби зі злочинами, які пов'язані з використанням комп'ютерної мережі, поняття про кіберзлочини розглядалося з точки зору двох аспектів: кіберзлочини в “широкому” і “вузькому” сенсі.

1. Кіберзлочин у вузькому сенсі (комп'ютерний злочин): будь-яке протиправне діяння, вчинене за допомогою електронних операцій, метою якого є порушення безпеки комп'ютерних систем і обробки ними даних.

2. Кіберзлочин у широкому розумінні (як злочин, пов'язаний із комп'ютерами): будь-яке протиправне діяння, вчинене за допомогою чи пов'язане з комп'ютерами, комп'ютерними системами або мережами, включаючи незаконне володіння і пропозицію чи розповсюдження інформації за допомогою комп'ютерних систем або мереж.

Разом із тим, у доповіді цього ж Конгресу вказується, що термін “комп'ютерні злочини” був розроблений для охоплення як абсолютно нових форм злочинності, орієнтованої на комп'ютери, мережі і їх користувачів, так і більш традиційних злочинів, які в даний час вчиняються з використанням або за допомогою комп'ютерного обладнання [10].

До того ж у виступі Генерального секретаря ООН “Висновки дослідження з питання про ефективні заходи щодо запобігання високотехнологічним та комп'ютерним злочинам і боротьби з ними” вживається термін “традиційні злочини”: *“Використання нових технологій у злочинних цілях призвело до виникнення абсолютно нових форм злочинності. З іншого боку, більш традиційні злочини в даний час вчиняються новими методами, які дають змогу збільшити вигоди або знизити ризики для злочинців”* [11].

Зарубіжні вчені, зокрема доктор Майк Макгуайр та Саманта Даулінг (Англія), також вважають, що кіберзлочинність є загальним терміном, що використовується для опису двох різних, але тісно пов'язаних між собою злочинних діянь: кіберзалежні та кіберутворюючі (злочини, пов'язані з кіберпростором).

Кіберзалежні – це злочини, які вчиняються з використанням комп'ютерів,

комп'ютерних мереж чи інших комунікаційних форм ІКТ. Такі, наприклад, як поширення вірусів та інших шкідливих програм, DDoS атаки, зламування серверів для захоплення мережевої інфраструктури або веб-сторінок. Кіберзалежні злочини спрямовані на пошкодження комп'ютерів та джерел мережі.

Кіберутворюючі (злочини, пов'язані з кіберпростором) – це традиційні злочини, масштаби яких збільшуються або досягаються за допомогою комп'ютерів, комп'ютерних мереж або інших ІКТ. На відміну від кіберзалежних злочинів, вони все ще можуть бути вчинені без використання ІКТ [12].

Отже, щодо класифікації кіберзлочинів, можна дійти висновку, що більшість дослідників, які вивчають проблему кіберзлочинності, пропонують поділяти кіберзлочини на види залежно від об'єкта та предмета посягання:

- нові злочини, що стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені розділом XVI Кримінального кодексу України);

- традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету.

В Україні найбільш повно статистичні дані про кіберзлочини відображаються у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України (у розд. XVII “Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції”, де, крім злочинів, окреслених розд. XVI КК України, зазначається ще низка інших злочинів, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 “Порушення авторського права і суміжних прав” і ст. 185 “Крадіжка”, чч. 3 і 4 ст. 190 “Шахрайство”, ст. 200 “Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення”, ст. 229 “Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару” і ст. 231 “Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю”, чч. 3, 4 і 5 ст. 301 “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів” КК України.

Крім цього, окремі показники про обліковані кіберзлочини, передбачені іншими статтями КК України, відображені в інших статистичних звітах, зокрема злочини, передбачені ст. 376-1 “Незаконне втручання в роботу автоматизованої системи документообігу суду” – в Таблиці 1.19 (“Злочини проти правосуддя”) у Єдиному звіті про кримінальні правопорушення, який готується Генеральною прокуратурою України (за 2019 рік обліковано 34 кримінальні правопорушення).

У розділі II “Участь служб та підрозділів Національної поліції у розкритті кримінальних правопорушень (за видами), досудове розслідування за якими закінчено” (Звіт про результати роботи підрозділів Національної поліції України (форма № 1-АВ)) кіберполіцією у 2019 році розкрито (розслідувано) кримінальних правопорушень, передбачених статтями КК України:

- ст. 156 “Розбещення неповнолітніх” – 15;

- ст. 191 “Привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем” – 16;

- ст. 357 “Викрадення, привласнення, вимагання документів, штампів, печаток, заволодіння ними шляхом шахрайства чи зловживання службовим становищем або їх пошкодження” – 11.

У розділі V “Відомості про окремі види кримінальних правопорушень, що зареєстровані у звітному періоді, та окремі показники результатів роботи по боротьбі з наркоманією” зазначено, що у 2019 році виявлено 421 факт збуту наркотичних засобів, психотропних речовин або їх аналогів, а також отруйних чи сильнодіючих речовин або отруйних чи сильнодіючих лікарських засобів із використанням всесвітньої мережі Інтернет.

Варто зазначити, що об’єктивна сторона, суб’єкт, суб’єктивна сторона, кваліфікований та особливо кваліфікований склад злочину, передбаченого ст. 301 КК України, у цілому збігаються з відповідними ознаками посягання, предметом якого є твори, що пропагують культ насильства і жорстокості (ст. 300 КК України). При цьому кримінальні правопорушення, передбачені ст. 301 КК України, вчинені з використанням високих інформаційних технологій, враховуються у звіті, а передбачені ст. 300 КК України – не враховуються.

Отже не всі традиційні злочини, що вчиняються за допомогою комп’ютерних технологій та Інтернету, відображаються у звітах як кіберзлочини.

Частина вітчизняних науковців до кіберзлочинів відносять злочини, передбачені статтями розділу XVI КК України та злочини, показники про які відображаються у звіті Національної поліції України “Звіт про результати роботи підрозділів Національної поліції України” (у розд. XVII “Відомості про кримінальні правопорушення, що вчинені з використанням високих інформаційних технологій, у тому числі виявлення і супроводження таких правопорушень працівниками підрозділів кіберполіції”).

Водночас деякі науковці, зокрема професор Савченко А.В., вважають, що крім кримінальних правопорушень, зазначених у вищевказаному звіті, під категорію кіберзлочинів можуть підпадати й інші злочини, передбачені КК України, за умови, що знаряддям їх вчинення будуть інформаційні мережеві технології та (або) їх наслідки позначатимуться у кіберпросторі [13].

До кіберзлочинів можуть належати такі злочини:

- дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109 КК України);
- посягання на територіальну цілісність і недоторканність України (ст. 110);
- державна зрада (ст. 111);
- диверсія (ст. 113);
- шпигунство (ст. 114);
- розголошення відомостей про проведення медичного огляду на виявлення зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби (ст. 132);
- незаконне розголошення лікарської таємниці (ст. 145); надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів референдуму, підсумків голосування або відомостей Державного реєстру виборців (в частині внесення неправдивих відомостей до бази даних Державного реєстру виборців, несанкціонованого втручання у роботу бази даних) (ч. 1 ст. 158);
- порушення таємниці голосування (ст. 159);
- порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (в частині пропаганди через Інтернет) (ст. 161);
- порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер (ст. 163);

- розголошення таємниці усиновлення (удочеріння) (ст. 168);
- порушення недоторканності приватного життя (ст. 182);
- розголошення комерційної або банківської таємниці (ст. 232);
- завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259);
- незаконне поводження зі зброєю, бойовими припасами або вибуховими речовинами (в частині збуту через Інтернет) (ст. 263);
- заклики до вчинення дій, що загрожують громадському порядку (ст. 295);
- ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300);
- сутенерство або втягнення особи в заняття проституцією (ст. 303);
- незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307);
- викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (ст. 312);
- викрадення, привласнення, вимагання обладнання, призначеного для виготовлення наркотичних засобів, психотропних речовин або їх аналогів, чи заволодіння ним шляхом шахрайства або зловживання службовим становищем та інші незаконні дії з таким обладнанням (в частині збуту через Інтернет) (ст. 313);
- розголошення державної таємниці (ст. 328); передача або збирання відомостей, що становлять службову інформацію, зібрану у процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни (ст. 330);
- погроза або насильство щодо працівника правоохоронного органу (ст. 345);
- погроза або насильство щодо журналіста (ст. 345–1);
- погроза або насильство щодо державного чи громадського діяча (ч. 1 ст. 346);
- погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов'язок (ч. 1 ст. 350);
- незаконне втручання в роботу автоматизованої системи документообігу суду (ч. 1 ст. 376);
- розголошення відомостей про заходи безпеки щодо особи, взятої під захист (ст. 381);
- розголошення даних оперативно-розшукової діяльності, досудового розслідування (ст. 387); погроза або насильство щодо захисника чи представника особи (ч. 1 ст. 398);
- розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422);
- пропаганда війни (ст. 436);
- виготовлення, поширення комуністичної, нацистської символіки та пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436.1).

Варто також вказати на існування певних проблемних питань кваліфікації кіберзлочинів. Як зазначають фахівці, основним критерієм відмежування злочинів, передбачених статтями 361 – 363-1 КК України, від інших злочинів, пов'язаних із використанням комп'ютерної техніки як знаряддя або засобу вчинення злочину, є об'єкт посягання. Так, особливістю кримінально-правової кваліфікації злочинів проти власності,

вчинюваних із використанням комп'ютерної техніки, визнається необхідність вирішення питання про доцільність додаткової кваліфікації дій винної особи за статтями, що передбачають відповідальність за злочини у сфері використання комп'ютерної техніки. Відповідаючи на це питання, слід керуватися тим, що використання комп'ютерної техніки при вчиненні злочинів проти власності утворює самостійний склад злочину лише тоді, коли заподіяно певну шкоду відповідному об'єкту – відносинам власності на комп'ютерну інформацію, коли певну інформацію було незаконно знищено, заблоковано, модифіковано. А в тих випадках, коли певні інформаційні системи використовуються за призначенням, додаткова кваліфікація не потрібна [14].

Також наразі існує проблема кримінально-правової кваліфікації дій, які користувачі комп'ютерів вчиняють у сфері обігу криптовалют та застосування штучного інтелекту.

Так, у березні 2018 р. дослідники з університету RWTH Aachen University (Німеччина) виявили, що блокчейн Bitcoin містить близько 1600 файлів, де є сцени жорстокого поводження з дітьми, при цьому не менше 8 файлів є порнографічним контентом. Блокчейн містить зовнішні посилання на 274 відеофайли, присвячені жорстокому поводженню з дітьми, та близько 142 посилань на darkweb. За словами вчених, знахідка може поставити блокчейн поза законом, водночас на сьогодні не існує жодних судових постанов з цього приводу, очевидно через складність кримінально-правової кваліфікації. Усі, хто бере участь у процедурі майнінгу або володіє біткоїнами, можуть бути причетними до появи порнографічного контенту в ланцюзі [15].

На практиці у працівників правоохоронних та судових органів виникає багато проблем щодо кваліфікації кіберзлочинів. Особливо це стосується випадків вчинення такого виду злочинів, що посягають на декілька об'єктів, охоронюваних кримінальним законом.

Найчастіше помилки зустрічаються при кваліфікації одного діяння, яке, на перший погляд, містить ознаки декількох складів злочинів. Отже, основною проблемою, вирішення якої впливає на правильність кваліфікації кіберзлочинів, є визначення наявності або відсутності у вчиненому ідеальної сукупності злочинів.

Під час вчинення кіберзлочину шкода може завдаватися: 1) суспільним відносинам, які виникають в ході забезпечення (за допомогою ІТС) життєдіяльності людини, суспільства, держави; 2) традиційним суспільним відносинам, охоронюваним кримінальним законом, які забезпечуються за допомогою ІТС; 3) традиційним суспільним відносинам, охоронюваним кримінальним законом, для нанесення шкоди яким використовуються ІТС, які, у свою чергу, не зазнають при цьому шкоди.

Перша група відносин охороняється розділом XVI Особливої частини КК України. Ці відносини є частиною другої та третьої групи відносин, але в другій групі вони зазнають шкоди разом із традиційними відносинами кримінально-правової охорони, а в третій – ні.

Ідеальною сукупністю злочинів вважається два або більше злочини, вчинені одним діянням. Відповідно до вказаних груп відносин, що зазнають шкоди при вчиненні такого діяння у випадку вчинення кіберзлочину, можна виділити три групи цих злочинів, що будуть мати свої особливості кваліфікації відповідно до діючого КК України: 1) злочини в сфері використання ЕОМ (комп'ютерів), їх систем, комп'ютерних мереж, мереж електрозв'язку; 2) злочини, що кваліфікуються за ст. КК України відповідно до об'єкту посягання з додатковим посиланням на статті розділу XVI ОЧ КК України; 3) злочини, що кваліфікуються за статтями КК України відповідно до об'єкту посягання без додаткового посилання на статті розділу XVI КК України.

Тобто діяння з першої та третьої групи є одиничними злочинами, а з другої – ідеальною сукупністю злочинів. Але в практиці застосування норм КК України в протидії кіберзлочинам діяння, що відносяться до різних із вказаних груп, часто плутаються. Найчастіше, злочини другої групи кваліфікуються тільки за однією статтею, і навпаки, злочини першої чи третьої групи кваліфікуються за декількома статтями, хоча не потребують додаткової кваліфікації. При цьому стаття, яка застосовується при кваліфікації другої групи злочинів, або із розділу XVI КК України, або інша – відповідно до безпосереднього об'єкту посягання. Очевидно, що в обох цих випадках частина злочину кваліфікацією не охоплюється, що порушує принципи повноти і точності кваліфікації, а у разі кваліфікації одного діяння, яке містить один склад злочину, за двома статтями порушується ще й принцип заборони подвійного інкримінування.

Як свідчить узагальнення судової практики, значна частка кіберзлочинів припадає на випадки, коли посягання в сфері використання ІТС здійснюється з корисливих мотивів з метою викрадення чи заволодіння чужим майном із заподіянням матеріальної шкоди і є способом вчинення таких злочинів проти власності, як шахрайство (ст. 190 КК України) або привласнення чи заволодіння майном шляхом зловживання службовим становищем (ст. 191 КК України). У більшості випадків суди кваліфікують такі дії за сукупністю злочинів: за статтею розділу XVI КК України і тією статтею, в якій передбачено відповідальність за конкретний злочин проти власності, способом здійснення якого було використання ІТС.

Наприклад, Печерський районний суд м. Києва визнав М. винним у тому, що він, працюючи провідним інженером відділу пластикових карток комерційного банку, як службова особа, що виконує адміністративно-господарські функції, зловживаючи своїм службовим становищем, маючи доступ до бази даних про клієнтів та їх рахунки, що містилась у його робочому комп'ютері, діючи з метою заволодіння грошовими коштами, виконав операцію з персоналізації сторонньої картки, скопіювавши на неї інформацію одного з клієнтів банку. З використанням картки-дубліката та банкоматів М. зняв і привласнив готівкою з рахунку клієнта грошові кошти на загальну суму 65 тис. 900 грн. Зазначені дії М. суд кваліфікував за ч. 4 ст. 191 КК України як заволодіння чужим майном шляхом зловживання службовим становищем, вчинене у великих розмірах. Крім того, суд кваліфікував дії М. ще й за сукупністю з ч. 3 ст. 362 КК України, оскільки М., будучи особою, яка мала право доступу до інформації, що оброблялася на комп'ютерах та зберігалася на носіях, несанкціоновано її скопіював, що призвело до витоку інформації і заподіяло значну шкоду.

Проте в деяких випадках суди кваліфікують зазначені дії лише за статтями розділу XVI Особливої частини КК України.

Так, Красногвардійський районний суд м. Дніпропетровська визнав Є. винним за ч. 1 ст. 361 КК України і призначив йому відповідне покарання. З матеріалів справи вбачається, що Є., діючи з корисливих мотивів, за допомогою спеціальних комп'ютерних програм створив дублікат-макет сайту компанії, яка спільно із ЗАТ КБ "ПриватБанк" надавала послуги з прискореного перерахування платежів за комунальні послуги і мобільний зв'язок через мережу Інтернет. У результаті такої діяльності Є. протягом певного часу викрадав грошові кошти з рахунків клієнтів ЗАТ КБ "Приват-Банк".

Автори узагальнення, з якого взяті ці приклади, вважають що в останньому випадку, оскільки Є. шляхом обману неодноразово заволодівав грошовими коштами за допомогою незаконних операцій з використанням ЕОМ, а втручання в роботу ЕОМ є способом вчинення злочину проти власності, то в цьому випадку зазначені дії потребують додаткової кваліфікації ще й за ст. 190 КК України (шахрайство). Вважаємо,

що тут дійсно наявна сукупність злочинів, але вона вже врахована в КК України в ч. 3 ст. 190, отже потрібна кваліфікація за цією нормою без додаткових посилань на норми КК України [16].

Одною із загальних проблем кримінально-правової кваліфікації є питання кваліфікації ідеальної сукупності злочинів, а саме поглинання одного злочину іншим, який був його частиною. Ця проблема досі потребує вирішення вченими.

Т.І. Созанський формулює правило стосовно злочинів, які мають додаткові об'єкти посягання: “Якщо ці об'єкти співвідносяться як основний і додатковий, то діяння кваліфікується як одиничний злочин, якщо ж обидва (чи більше) об'єкти є основними, то діяння утворює ідеальну сукупність злочинів”. Але далі він вказує, що визначити, коли об'єкт є додатковим, а коли він переходить у основний, особливо при оцінці кіберзлочину, доволі складно. Він пропонує, як один із варіантів вирішення цього питання, визначати суспільну небезпечність посягань на відносини, які охороняються цими об'єктами. Якщо суспільна небезпечність відносин, що охороняються додатковим об'єктом, є більшою, ніж основного об'єкта, то діяння утворює ідеальну сукупність [17].

У практичну площину цю рекомендацію перевів Пленум Верховного Суду України у постанові, яка стосується судової практики застосування норм про множинність злочинів. У п. 11 цієї постанови вказано: “Якщо у складі злочину передбачене діяння, яке у поєднанні з іншими обставинами завжди утворює склад іншого злочину, то питання про його кримінально-правову оцінку необхідно вирішувати з урахуванням того, наскільки охоплюється складом цього злочину таке діяння, а також з урахуванням змісту санкцій відповідних статей (частин статей) ОЧ КК України. У випадках, коли складом певного злочину охоплюється вчинене одночасно з цим злочином відповідне діяння і санкцією статті (частини статті) ОЧ КК України встановлене за цей злочин більш суворе максимальне основне покарання, ніж за відповідне діяння, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує”.

Таким чином, слід визнати за правило кваліфікації кіберзлочинів, які через посягання на відносини в сфері використання ІТС посягають на інші “традиційні” відносини, які забезпечуються цими ІТС, наступне: у разі, коли складом певного злочину охоплюється вчинене одночасно з цим злочином діяння, передбачене статтею Розділу XVI і санкцією статті (частини статті) КК України встановлене за цей злочин більш суворе максимальне основне покарання, ніж за діяння, передбачене статтею Розділу XVI КК України, таке діяння не утворює сукупності злочинів і окремої кваліфікації не потребує.

Висновки.

Сьогодні офіційного, закріпленого в міжнародних документах визначення кіберзлочинності поки не існує. Класифікації кіберзлочинів, які надаються в офіційних документах, зокрема ООН, ЄС, та дослідженнях науковців, через які розкривається поняття кіберзлочинності також різняться.

У вітчизняному законодавстві нині також не існує чіткого визначення поняття кіберзлочину. Дискутуються різні точки зору щодо класифікації кіберзлочинів. Відсутній перелік “традиційних” злочинів, які можуть відноситися до категорії кіберзлочинів, а отже і відсутня офіційна статистична звітність щодо облікованих кіберзлочинів.

Отже, сьогодні є нагальна потреба визначитися з переліком “традиційних” злочинів, які можуть відноситися до категорії кіберзлочинів, внести зміни до відомчої статистичної звітності Національної поліції України.

Аналіз такої статистичної звітності надав би можливість проаналізувати динаміку цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів та розробляти на їхній основі організаційно-правові заходи для більш ефективної протидії кіберзлочинності на національному рівні. Зокрема, для протидії вчиненню “традиційних” злочинів з використанням мережі Інтернет, відповідальність за які передбачена Кримінальним кодексом України, необхідно розробити методичні рекомендації щодо кримінально-правової кваліфікації “традиційних” злочинів, вчинених з використанням мережі Інтернет.

Використана література

1. Про основні засади забезпечення кібербезпеки України: Законі України від 05.10.17 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
2. Ахтирська Н.М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *ПРАВО*. – (Наук. вісник Ужгородського націон. ун-ту). 2016. Вип. № 36. С.123-126.
3. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій: навч. посіб. / В.М. Бутузов та ін. – (Рада нац. безпеки і оборони України, Міжвід. наук.-дослід. центр з проблем боротьби з організованою злочинністю, Служба безпеки України, Нац. акад. СБУ). Київ, 2011. 404 с.
4. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя: Гуманітарний ун-т “ЗІДМУ”, 2003. 296 с.
5. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі “Даркнет”. *Інформація і право*. № 3(26)/2018. С. 111-117. URL: http://nbuv.gov.ua/UJRN/In_fpr_2018_3_13
6. Демедюк С.В., Марков В.В. Кіберполіція України. *Наше право*. 2015. № 6. С. 87-93. URL: http://nbuv.gov.ua/UJRN/Nashp_2015_6_15
7. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2012. Вип. 1. С. 312-320. URL: http://nbuv.gov.ua/UJRN/boz_2012_1_37
8. Столяр О. Міжнародно-правові проблеми визначення та класифікації “кіберзлочинів”. URL: <http://www.jurnaluljuridic.in.ua/archive/2017/4/43.pdf>
9. Home Affairs Committee E-crime Fifth Report of Session 2013–14. URL: <https://publications.parliament.uk/pa/cm201314/cmselect/cmhaff/70/70.pdf>
10. Joint communication to the European parliament, the Council, the European economic and social committee and the committee of the regions. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 02.2013. URL: <http://eur-lex.europa.eu/legal-content/EN/NOT/?uri=celex:52013JC0001>
11. Десятый Конгресс Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями. м. Вена, 10 – 17 апреля 2000 года. URL: https://digitallibrary.un.org/record/432663/files/A_CONF.187_15-RU.pdf; https://digitallibrary.un.org/record/432653/files/A_CONF.187_10-RU.pdf?version=1
12. Экономический и Социальный Совет ООН. Комиссия по предупреждению преступности и уголовному правосудию. м. Вена, 8 – 17 мая 2001 года. URL: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjGip3Ys8DfAhXQp4sKHTltB9wQFjAAegQICBAC&url=https%3A%2F%2Fwww.unodc.org%2Fdocuments%2Fcommissions%2FFCCPCJ%2FFCCPCJ_Sessions%2FFCCPCJ_10%2FE-CN15-2001-04%2FE-CN15-2001-4_R.pdf&usg=AOvVaw1dtJrz_5oLSWMd4q4AwGnb
13. Dr. Mike McGuire and Samantha Dowling Cybercrime: A review of the evidence Summary of key findings and implications. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

14. Науково-практичний коментар Закону України “Про основні засади забезпечення кібербезпеки України” / М.В. Гуцалюк та ін.; за ред. М.В. Гребенюка. Київ: Національна академія прокуратури України, 2019. 220 с.

15. У блоках Bitcoin виявили сліди дитячої порнографії. URL: <https://www.Volynnews.com/news/all/u-blokakh-Bitcoin-vyiavyly-slidy-dytiachoyi-pornohrafiyi->

16. Узагальнення щодо кваліфікації сукупності злочинів. – (Опрацьовано суддею Верховного Суду України М.І. Грицівим та головним консультантом управління вивчення та узагальнення судової практики Верховного Суду України В.В. Антощуком). URL: [http://www.viaduk.net/clients/vsu/vsu.nsf/\(documents\)/AFB1E90622E4446FC2257B7C00499C02](http://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02)

17. Созанський, Т.І. Кваліфікація сукупності злочинів: автореф. дис. ...канд. юрид. наук : 12.00.08. – (Львів. держ. ун-т внутр. справ). Львів, 2009. 18 с.

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

УДК 351.746

**СТРЕЛЬБИЦЬКА Л.М.**, доктор юридичних наук, професор, завідувач кафедри цивільно-правових дисциплін НА СБ України.

**СТРЕЛЬБИЦЬКИЙ М.П.**, доктор юридичних наук, професор, головний науковий співробітник наукової лабораторії НОЦ НА СБ України.

## **МЕТОДОЛОГІЧНІ ТА ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ФОРМУВАННЯ І ФУНКЦІОНУВАННЯ СИСТЕМИ ДЕРЖАВНОГО УПРАВЛІННЯ НАЦІОНАЛЬНОЮ БЕЗПЕКОЮ УКРАЇНИ**

**Анотація.** В статті досліджуються питання методологічних та організаційно-правових засад формування і функціонування системи державного управління національною безпекою України. Аналізуються нормативно-правові акти, що регулюють питання державного управління національною безпекою України, його стан та шляхи покращення. Головні напрями удосконалення управління національною безпекою розглядаються через такі найважливіші підходи як організаційно-правовий; процесний; системний; ситуаційний. За змістом ці підходи поєднуються в мистецтво і науку управління. Проблеми державного управління в контексті інформаційної та гібридної війн аналізуються з позицій юридичної та управлінської науки, які сьогодні розроблені та висвітлені недостатньо, у зв'язку з чим Україна дорогою ціною платить за прорахунки й відсутність державної управлінської та кадрової політики в період незалежного державотворення. Більше того, сучасна гібридна та інформаційна війна вийшла на новий, більш високий рівень і тепер уже реально загрожує всій національній безпеці та територіальній цілісності Української держави, що потребує адекватних коректив системи управління національною безпекою, на що звернуто особливу увагу у статті. Охарактеризовано методологію оцінки стану управління національною безпекою, яка мусить забезпечувати необхідний рівень захищеності корінних інтересів людини й громадянина, суспільства й суверенної держави в цілому від явних і потенційних внутрішніх та зовнішніх загроз, їхнього своєчасного виявлення, запобігання і нейтралізації, що гарантує стабільний всебічний прогрес, стійкий розвиток суспільства.

**Ключові слова:** національна безпека, види безпеки, державне управління, суб'єкти, об'єкти управління, внутрішні, зовнішні загрози національній безпеці України.

**Summary.** The article highlights the questions of methodological and organizational and legal bases of formation and functioning of the system of state management of national security of Ukraine. The legal acts regulating the issues of state administration of national security of Ukraine, its state and ways of improvement are analyzed. The key areas of improvement of national security management are considered through the prism of the following crucial approaches: organizational and legal; process; systemic; situational. These approaches' background are put together into the art and science of management. Problems of government in the context of information and hybrid wars are analyzed from the standpoints of legal and administrative science, which are not sufficiently developed and covered today, in this connection, Ukraine pays a very high price for miscalculations and lack of state management and HR policy in the period of independent state formation. Moreover, the modern hybrid and information war has reached a new, higher level, and now it constitutes a real danger to the whole national security and territorial integrity of Ukraine. That needs adequate adjustments to the national security management system, which is emphasized in the article. The methodology for assessing the state of national security management, which should provide the necessary level of protection of the indigenous interests of the individual and the citizen, society and the sovereign state as a whole from the obvious and potential internal and external threats, their timely detection, prevention and neutralization, which guarantees a stable and multifaceted progress, permanent development of the society.

**Keywords:** *national security, types of security, public administration, subjects, objects of management, internal, external threats to the national security of Ukraine.*

**Аннотация.** В статье исследуются вопросы методологических и организационно-правовых принципов формирования и функционирования системы государственного управления национальной безопасностью Украины. Анализируются нормативно-правовые акты, регулирующие вопросы государственного управления национальной безопасностью Украины. Главные направления совершенствования управления национальной безопасностью рассматриваются через такие важнейшие подходы как организационно-правовой; процессный, системный; ситуационный. За содержанием эти подходы соединяются в искусство и науку управления. Проблемы государственного управления в контексте информационной и гибридной войн анализируются с позиций юридической и управленческой науки, которые сегодня разработаны и освещены недостаточно, в связи с чем Украина дорогой ценой платит за просчеты и отсутствие управленческой и кадровой политики в период государственной независимости. Более того, современная гибридная и информационная война вышла на новый, более высокий уровень и теперь уже реально угрожает всей национальной безопасности и территориальной целостности Украинского государства, что потребует адекватных корректив управления национальной безопасностью, на что обращено особое внимание в статье. Дана характеристика методологии оценки состояния управления национальной безопасностью, которая должна обеспечивать необходимый уровень защищенности коренных интересов человека и гражданина, общества и суверенного государства от явных и потенциальных внутренних и внешних угроз, их своевременного выявления, предупреждения и нейтрализации, что гарантирует стабильный всеобщий прогресс, устойчивое развитие общества.

**Ключевые слова:** *национальная безопасность, виды безопасности, государственное управление, субъекты, объекты управления, внутренние, внешние угрозы национальной безопасности Украины.*

**Постановка проблеми.** Успішне існування незалежної України можливе лише за умови надійного управління національною безпекою та її окремими видами. Державне управління національною безпекою України здійснюється шляхом цілеспрямованого впливу комплексного суб'єкту (системи державних органів влади та управління) на об'єкт управління з метою належного забезпечення національної безпеки.

Об'єктом управління в даному випадку виступає національна безпека України, якою згідно із пп. 9-10 ст. 1 Закону України "Про національну безпеку України" є захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз. Національні інтереси України визначаються як життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян [1].

Фахівці неодноразово підкреслювали, що національна безпека України сьогодні перебуває у найскладнішому стані з часів незалежності держави. Зросли і ускладнились її зовнішні та внутрішні загрози. До реальних загроз вже відносяться зовнішнє втручання, гібридна війна, втрата територій України, політична та владна корупція, які призвели до відчутних і непоправимих наслідків. В основі національної безпеки лежить відповідальна і виважена державна політика відповідно до прийнятих доктрин, стратегій, концепцій і програм у таких сферах як політична, економічна, соціальна, воєнна, екологічна, науково-технологічна, інформаційна тощо[2, с. 27].

Комплексне дослідження і розв'язання проблем управління у сфері національної безпеки дасть можливість здійснити подальшу розбудову цього інституту в напрямі

його адаптації до вимог Європейського Союзу, створити ефективну систему управління, яка б відповідала стандартам демократичної, правової держави, проголошеної Конституцією України. Значною мірою це залежить від керівного та кадрового складу державної служби України і потребує прискореного реформування та розвитку її управлінської ланки, залучення на всіх рівнях до системи управління керівних кадрів нової генерації: професійно підготовлених, компетентних, патріотично налаштованих, чесних, порядних, відповідальних, енергійних та ініціативних. У зв'язку з цим проблема управління у сфері національної безпеки набуває особливого значення.

**Результати аналізу наукових публікацій.** Системне й усебічне вивчення проблеми державного управління сферою національної безпеки зумовлює необхідність аналізу стану її наукової розробки не лише вітчизняними, але й зарубіжними вченими, які здійснювали свої дослідження в галузях права, політології, державного управління, економіки, психології, соціології, менеджменту тощо. Такий аналіз дає змогу узагальнити досягнуті в цій сфері результати та визначити шляхи подальших наукових пошуків.

Сучасні погляди на проблеми методології, організаційно-правових засад формування і функціонування системи державного управління національною безпекою, практичного вирішення питань державного управління викладені в працях В.Б. Авер'янова, В.Д. Бакуменка, В.Г. Бодрова, В.М. Князева, С.М. Князева, Б.В. Литова, В.І. Лугового, В.Я. Малиновського, О.Г. Мордвінова, С.П. Мосова, П.І. Надолішнього, Н.Р. Нижник, В.А. Ребкала, В.М. Рижих, Г.П. Ситніка, С.М. Серьогіна, В.О. Шамрая та ін.

Водночас, аналіз сучасної наукової літератури з проблем державного управління свідчить про те, що в науковому розумінні питання про систему управління у сфері національної безпеки на сьогодні залишається малодослідженим. Теоретико-методологічні засади її формування та організації функціонування розглядаються епізодично, в межах самотійних видів, без системного, комплексного й цілісного підходу, оцінки стану національної безпеки, науково обґрунтованих висновків, пропозицій і рекомендацій по її поліпшенню, особливо в умовах глобальної гібридної та інформаційної війни.

**Метою статті** є визначення передумов наукового формування та ефективного функціонування системи управління національною безпекою України.

**Виклад основного матеріалу.** Теорія національної безпеки на цей час ще знаходиться в стадії розробки. Вітчизняні управлінці поки що в основному обмежуються обґрунтуванням лише теоретичних положень забезпечення національної безпеки в окремих її сферах (політичній, державній, інформаційній, економічній та інших), а фундаментальних наукових досліджень проблеми комплексного управління ефективним забезпеченням національної безпеки з позицій системного підходу бракує. Як наслідок, відсутні загальноприйняті погляди щодо понятійно-категорійного апарату в галузі національної безпеки, мають місце досить суперечливі погляди щодо життєво важливих національних інтересів, подальших напрямків державного будівництва, раціональної структури та управління сектором безпеки, а відтак і методів, засобів, способів та механізмів реалізації державної політики з питань національної безпеки.

Зазначене вимагає від політиків і державних службовців пошуку принципово нових ідей, політичних і державно-управлінських рішень, удосконалення існуючих та створення нових механізмів щодо забезпечення національної безпеки, а від науковців – подальшого розроблення і доопрацювання теоретико-методологічних основ забезпечення національної безпеки крізь призму осмислення сучасних поглядів на сутність, шляхи, засоби, способи і методи захисту національних інтересів.



Процеси радикального оновлення українського суспільства та правоохоронної системи, що відбуваються на сучасному етапі державотворення в Україні, ставлять підвищені вимоги до системи управління у сфері національної безпеки. Проблеми управління в державі є наслідком тієї кадрової ситуації, що складалася протягом тривалого часу в Україні і характеризується низьким професіоналізмом, відсутністю спеціальної управлінської підготовки, невідповідністю фахової підготовки профілю діяльності, бюрократизмом, байдужістю і тотальною корумпованістю керівних кадрів. Як наслідок, усе це призводить до нераціонального, малорезультативного й неефективного управління на державному, регіональному, відомчому та місцевому рівнях.

Управління у сфері національної безпеки України є галузевим різновидом державного управління, що, у свою чергу, розглядається як один із видів соціального управління. Його особливістю є те, що діяльність здійснюється у великих масштабах, потребує адекватного управління, яке являє собою узгодженість між індивідуальними та груповими діями і реалізується через загальні функції держави, що виникають зі спільної соціально-політичної та економічної ситуації. Рівень ефективності вирішення вказаних завдань в умовах складних політичних, соціальних, економічних та воєнних процесів, наявних загроз національній безпеці прямо залежить від як дієвості самого управління, так і стану системи управління нею, управлінського професіоналізму її керівників і виконавців. Становлення та розвиток теорії управління в сфері національної безпеки здійснюється не тільки шляхом проведення традиційних наукових досліджень, але й всебічного вивчення управлінської практики, динаміки суспільно-політичних подій.

Цінність управління як виду професійної діяльності полягає в тому, що це єдиний вид суспільної і, власне, управлінської практики, який перетворює безпосередньо потенціал наукових знань про професійні можливості людини на практичну сферу діяльності, стаючи одночасно і важливим чинником, і ресурсом управління суспільством, державою, організацією, їх стабільного розвитку. Предметна сфера діяльності управління національною безпекою така, що її науково-теоретична база має синкретичний та інтегративний характер, а тому її можна віднести до спеціальностей складного управлінського профілю.

Як визначав директор інформаційних сил Міністерства оборони США: «Інформаційна війна складається із дій, що застосовуються для досягнення інформаційної переваги в забезпеченні національної воєнної стратегії шляхом впливу на інформацію та інформаційні сили супротивника з одночасним захистом та зміцненням нашої власної інформації та інформаційних систем. Інформаційна війна являє собою всеохоплюючу, цілісну стратегію, призначену віддати належне значенню та цінності інформації у питаннях командування й управління збройними силами і реалізації національної політики» [3].

У контексті цієї проблеми слід розглянути, що являє собою Україна та її державна інформаційна політика. У всіх подіях, що нині відбуваються в нашій державі, починаючи із захоплення й анексії Криму, особливо з перших часів воєнного конфлікту на сході, Україна не змогла нічого суттєвого протиставити в цій інформаційній війні. Те ж можна сказати і щодо готовності Збройних Сил України до участі й проведення воєнних дій. Природа цих чинників практично однакова. Інформаційний ресурс щодо реальних зовнішніх та внутрішніх загроз Україні, для прийняття адекватних управлінських рішень, як неодноразово підкреслював виконуючий обов'язки Президента України Турчинов О.В., тоді був відсутній.

Як свідчить вітчизняний досвід, розвиток молодій державі повинні були регулювати не стільки політичні сили, скільки структури державного управління на відповідних організаційних та правових засадах, ігнорування яких спроможне знищити саму національну державність. Основу такого управління мала формувати його найголовніша складова – управління національною безпекою. Це, на жаль, вдавалося не завжди. У зв'язку з цим уже протягом перших років існування самостійної української держави чітко визначилися, на нашу думку, принаймні п'ять груп негативних тенденцій, наявність яких у свій час й було розкрито, але належних висновків і заходів вжито не було:

- підміна державної управлінської діяльності політичною боротьбою численних течій, груп, окремих осіб за відстоювання власних вузьких (регіональних, ідейних, особистих) інтересів, у яку були втягнуті як законодавча, так і виконавча влада, державні управлінські структури, що ставали засобом досягнення групових і приватних цілей, серед яких “розчинились” інтереси держави та основної частини її трудового населення;

- як наслідок протистояння централізованому управлінню в період розпаду СРСР, активного поширення набув процес дезінтеграції, перерозподілу влади між центром і регіонами, що було об'єктивною необхідністю саме за тих умов, проте пізніше переросло в боротьбу за повну управлінську, економічну та іншу незалежність від усіх структур, що існують “понад ...”, і породило сепаратизм;

- оскільки прийоми політичної боротьби були перенесені до сфери державного управління й економіки, зміна форм власності і власника, структурна перебудова економіки призвели до масового банкрутства і зупинки багатьох потужних виробничих підприємств, а отже, і до різкого падіння рівня життя основної маси населення й появи за рахунок цього “нுவоришів”;

- втрата роботи й колишніх загальних соціальних гарантій підштовхувала значну частину активного населення до пошуку самостійного виходу із важкого становища, головним чином, двома шляхами – пошуку будь-яких засобів існування, включаючи злочинні дії маргінальних прошарків населення, або за допомогою акцій непокори і протесту більш освіченої й організованої його частини, які часто змішувалися між собою, спрямовуючи свої зусилля проти повалення влади;

- за останні 50 років значно погіршився екологічний стан України: гігантська забудова шкідливими промисловими підприємствами й атомними станціями, Чорнобильська катастрофа... Наслідки цього доведеться ліквідовувати зусиллями ще не одного покоління. І, здавалося б, у таких умовах повинна взяти гору загальна генетична зацікавленість людей у виживанні. Але цього не сталося.

На фоні цих тенденцій був спотворений і скомпрометований процес приватизації, на який усі покладали так багато надій, сприймаючи його як можливість одержання економічної незалежності кожним, засіб покращення свого матеріального становища. І надії ці не були безпідставні: на час розпаду СРСР Україна мала найвищий економічний потенціал на одного жителя, виробляла 5 % обсягу світової продукції при 0,8 % населення Землі, сприятливі природні, виробничі та інші умови, 25 % світових площ чорнозему. Зазначене давало змогу багатьом експертам передбачати і стверджувати, що Україна має можливість першою серед держав СНД вийти з економічної кризи. Проте сталося навпаки. Одні “заговорили країну”, інші – ошукали, відправивши награбоване за кордон, а треті, і таких переважна більшість, розділили долю країни, описавши траєкторію її руху від бідності до злиднів [4].

Не було чіткості й у визначеності шляху розвитку. Потребували вивчення і коригування, враховуючи наші національні особливості, історична практика та світовий досвід державотворення. У багатьох представників керівних структур були відсутні практичні навички самостійного управління державою взагалі і в критичних умовах, зокрема. На початковій стадії державотворення сумлінну працю підмінювали популізмом, а соціально-економічне облаштування суспільства – атрибутивною розбудовою держави, корумпованими діями. Видавши масу нормативних документів щодо боротьби з корупцією, влада сама стала її носієм, а потім і її жертвою. Тому через тривалий час існування незалежної України виникла ідея люстрації як необхідності перевірки й очищення влади, вже пострадянської. Але на ділі, як потім показали порушені справи і результати діяльності НАБУ, люстрація лише “розчистила дорогу” новому поколінню ненаситних корупціонерів.

Із часу незалежності України з 1991 р. виросло нове покоління її громадян, які сьогодні складають основу працездатного населення. Воно формувалось і виховувалося в умовах боротьби за державну незалежність, у новому інформаційному середовищі, має свої ідеали й орієнтири, зокрема на європейські стандарти життя, не рахуватися з якими небезпечно. Ці молоді люди, як свідчить преса, приходять і бачать світ, який їм не належить: банки, в яких у них немає рахунків; автомобілі, що їздять по вулицях і в яких сидять не вони; поділені земельні ділянки та підприємства, власниками яких є інші люди (окрім дітей корупціонерів та олігархів). Це покоління часто залишається не поміченим.

Із безпекових спостережень можна зробити висновок, що сьогодні загрози національній безпеці молодій державі змістилися переважно із внутрішніх до зовнішніх. Якщо (майже до кінця 2013 р.) доля України залежала від неї самої, її внутрішніх чинників, якими можна було управляти без зовнішнього втручання, то з початку 2014 р. її доля вже значною мірою вирішується за межами держави, інколи за участю ООН, інших міжнародних та європейських інституцій. Суттєву роль у внутрішніх загрозах, що виникли, відіграють прорахунки окремих гілок влади, що є суб'єктами забезпечення національної безпеки.

У сучасних умовах всі гілки влади мусять об'єднатися задля реалізації ідей, проголошених революцією гідності, що прямо залежить від стану інформаційної безпеки. Завдяки демократії ми маємо сьогодні багатоманітність суспільної думки, поглядів людей. І тепер на цьому фоні мусимо забезпечити ще і єдність нації, від чого вирішальною мірою залежить стан національної безпеки. Сучасна вітчизняна парадигма єдності нації вимагає від кожного уміння відрізнити справжні національні інтереси від удаваних, надуманих, кланових, що видаються за національні. Реалізація національних інтересів народу після здобуття незалежності забезпечує, насамперед, стабільність, благополуччя, спокій, еволюційний розвиток держави та нації тощо.

Національна безпека неможлива без міцної держави, стійкості центральної влади та стабільності суспільства. Забезпечення національної і державної безпеки повинно здійснюватися за відповідними складовими, ядро й основу яких складає економічна й фінансова безпека.

Складові національної безпеки не можуть бути стандартними або загальноприйнятими для всіх країн. Вони залежать від того, в якому стані розвитку чи занепаду перебуває держава. Наприклад, Рада національної безпеки США орієнтована на вирішення проблем захисту власних національних інтересів США на всесвітньому рівні. В Україні ж багаторічна внутрішня криза потребує насамперед зосередження сил на вирішенні широкого кола внутрішніх проблем.

Сьогодні вже можна говорити про наявність теорії національної безпеки. Теорія національної безпеки – це меганаука, що поєднує в собі прикладні аспекти правових, соціальних, воєнних, гуманітарних, технічних, психологічних, біологічних та інших наук з метою дослідження суті, змісту, методів, форм і засобів забезпечення безпеки особистості і соціальних спільнот різного рівня [5, с. 7].

Останнім часом у гуманітарних науках помітного значення набуває сфера безпекознавства, що обумовлено глобальними загрозами світовій цивілізації і людству а також необхідністю залучення вчених до вироблення адекватних заходів захисту. У першу чергу це стосується України, її національної, державної, прикордонної, управлінської, кадрової, економічної, кібернетичної, інформаційної, енергетичної, духовної, релігійної, продовольчої, медичної, громадської, екологічної, біологічної, фінансової, банківської, соціальної, воєнної, внутрішньо-політичної, гуманітарної, демографічної, правової, техногенної, радіологічної, регіональної, пожежної, зовнішньо-політичної і міжнародної безпеки. Як бачимо, наведена розгалуженість нараховує 30 основних видів безпеки, які у тій чи іншій мірі вітчизняними науковцями раніше досліджувались. Цей перелік не претендує на вичерпність і потребує методологічного та теоретичного узагальнення у межах окремої науки безпекознавства, спробу якого зроблено авторами статті. Перш за все, види безпеки систематизовано за єдиним критерієм, залежно від суб'єктів, на які покладені обов'язки із забезпечення цих видів безпеки та контролю за ними. Насамперед, це стосується національної і державної безпеки, які забезпечуються державою, її законодавчою, виконавчою і судовою владою, міністерствами, відомствами України. До неї також належать: конституційна, антитерористична, прикордонна, управлінська, кадрова, економічна, кібернетична, інформаційна (захист “закритої” інформації), національно-культурна; демографічна, енергетична, функціонування об'єктів критичної інфраструктури; воєнна, гуманітарна, зовнішньо-політична і міжнародна безпека тощо.

Окрім цього, відносно самостійно сформувалась безпека особистої та колективної життєдіяльності, яка охоплює такі види безпеки, як: медична, охорони здоров'я, генетична, психологічна, соціальна, антикримінальна, антинаркотична, техногенна, виробнича, побутова, транспортна, протипожежна, духовна, просвітницько-виховна, продовольча, природна, екологічна, хімічна, біологічна, фінансова, банківська, підприємницька, інвестиційно-іноваційна; радіологічна, регіональна, технологічна, соціокультурна тощо.

Наявні також види безпеки, які забезпечують політичні партії, громадські, релігійні організації, спілки, асоціації: внутрішньо-політична, громадська, релігійна безпека тощо.

Завершує систему класифікації видів безпеки підсистема міжнародної колективної безпеки (ООН, ЄС та інші міжнародні інституції) від глобальних всесвітніх та зовнішніх загроз: антивоєнна, протиепідемологічна, міжнародна антитерористична, загального клімату, протиастероїдна тощо.

Унаслідок такої систематизації ми вже нараховуємо майже 50 видів безпеки. І це ще не межа! Все це свідчить про необхідність не лише кваліфікації видів безпеки за одними і тими ж критеріями, створення єдиної системи, але і про доцільність вироблення механізму управління цією складною і важливою для світу безпековою системою, своєчасного виявлення реальних загроз, викликів і ризиків.

Не маючи на меті всебічне дослідження феномену національної безпеки, якому вже приділено достатньо уваги, торкнемося лише загальнотеоретичних та практичних її аспектів, від яких залежить державне управління сферою національної безпеки України.

Питання розробки та стану національної безпеки є фундаментальним і багато в чому визначає напрям та перспективи розвитку держави, суспільства й кожної окремої особистості. В умовах відсутності національної єдності “становище ускладнюється тим, що в суспільстві існують різноманітні конкуруючі тлумачення національних інтересів національної безпеки різними соціальними групами. Це об’єктивно призводить до соціальної напруженості та конфліктів, знижує загальний рівень безпеки усіх без винятку соціальних груп” [6, с. 12].

Ще більше окремі вчені критикували характеристику стану національної безпеки і практичних дій з її забезпечення вже в перші роки незалежності, підводячи до невтішного прогнозу: “Успішно проваливши всі спроби проведення економічної, адміністративної та військової реформи (чи, точніше буде сказати, спроби імітації цих реформ), опинившись після 11 років незалежності серед найбідніших країн-маргіналів Європи (з ВВП на рівні вартості щорічної продукції транснаціональної компанії “Siemens”), Україна сьогодні не здатна забезпечити необхідного рівня безпеки для своїх громадян як на індивідуальному, так і на соціальному рівнях [7].

Комплексний підхід до розгляду організаційних та правових засад державного управління обумовлений сучасними терористичними та сепаратистськими загрозами національній безпеці незалежної України, які посягають на її суверенітет і територіальну цілісність. Це вимагає мобілізації зусиль усіх суб’єктів безпекового сектору України й удосконалення управління ними. Діяльність органів державного управління у сфері національної безпеки має досить складний характер, що пояснюється наявністю особливих об’єктів безпеки: особистість, суспільство й держава, – проти яких сьогодні спрямована розвідувально-підбивна діяльність окремих країн із подальшими бойовими діями.

Як стверджує професор Ю.П. Битяк, в адміністративно-правовій теорії та практиці державного управління до сфери адміністративно-політичної діяльності належать такі галузі, як національна безпека, оборона, внутрішні справи, закордонні справи, юстиція. Органи управління цими галузями є елементами єдиної системи державного управління, стосуються органів виконавчої влади й активно здійснюють функції держави. Особливе місце в цій системі посідають національна безпека та органи, що здійснюють управління нею. Сьогодні ще не існує чіткого механізму діяльності органів державного управління у сфері національної безпеки, але безперечним є те, що національна безпека України є об’єктом державного управління [8].

Склад сектору безпеки і оборони (суб’єкт) забезпечення національної безпеки є досить різноманітним. Його, а також покладені на нього управлінські функції визначено у розділі IV Закону України “Про національну безпеку України” [1], де “Основні положення” зводяться до наступного. Сектор безпеки і оборони України складається з чотирьох взаємопов’язаних складових (ст. 12): сили безпеки; сили оборони; оборонно-промисловий комплекс; громадяни та громадські об’єднання, які добровільно беруть участь у забезпеченні національної безпеки. Функції та повноваження окремих складових сектору безпеки і оборони визначаються Законом України “Про національну безпеку України” [1] та чинним законодавством України.

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.

Інші державні органи та органи місцевого самоврядування здійснюють свої функції із забезпечення національної безпеки у взаємодії з органами, які входять до складу сектору безпеки і оборони.

Управління та керівництво у сферах національної безпеки і оборони здійснюється у відповідності до ст. 13 зазначеного закону. Загальне керівництво у сферах національної безпеки і оборони відповідно до Конституції України здійснює Президент України.

Управлінську функцію координації у сферах національної безпеки і оборони здійснює Рада національної безпеки і оборони України відповідно до ст. 107 Конституції України та ст. 14 Закону України “Про Раду національної безпеки і оборони України”. В умовах воєнного або надзвичайного стану, в особливий період, а також у разі виникнення кризових ситуацій, що загрожують національній безпеці України, Рада національної безпеки і оборони України координує діяльність органів виконавчої влади, розглядає пропозиції щодо застосування відповідно до закону спеціальних економічних та інших обмежувальних заходів.

Кабінет Міністрів України як вищий орган у системі органів виконавчої влади вживає заходів щодо забезпечення обороноздатності, національної безпеки й боротьби зі злочинністю. У межах визначеної законом компетенції забезпечує: управління державними органами у сфері національної безпеки; організовує й контролює розробку та реалізацію заходів щодо її гарантування міністерствами і відомствами, іншими підпорядкованими йому органами України.

Конституційний Суд України вирішує питання про відповідність законів та інших правових актів у сфері національної безпеки Конституції України й дає офіційне їх тлумачення.

Суди загальної та спеціальної юрисдикції здійснюють правосуддя у сфері забезпечення національної безпеки.

Прокуратура України здійснює наглядові повноваження у сфері національної безпеки.

Національний банк України розробляє та здійснює емісійно-кредитну політику в інтересах національної безпеки.

### **Висновки.**

Залежно від критеріїв класифікації, основу яких складають сутність, походження та нормативно-правове оформлення, засади управління національною безпекою складають дві великі групи: організаційні та правові.

До *організаційних* належать такі: відомчість, лінійність, функціональність, чітке підпорядкування, централізм управління, оперативність керівництва, раціональний розподіл повноважень, персональна відповідальність, поєднання колегіальності і єдиноначальності, головна ланка, адекватність оперативних сил і засобів особливостей і динаміці оперативної обстановки, відповідності кадрової політики покладеним завданням; розмежування сфер діяльності оперативних органів, взаємодії і координації їх діяльності; незалежність та оперативність у поданні оперативної інформації; гарантованість права на інформацію; доступність відкритої інформації та свобода її обміну; об’єктивність, вірогідність інформації; повнота і точність інформації; законність одержання, використання, поширення та зберігання інформації; опора на громадськість; конкретність; оптимальність; ефективність.

*Правові засади* управління національною безпекою України – це єдність конституційних, законодавчих, адміністративно-правових та відомчих нормативних актів, які встановлюють, змінюють або відновлюють правовідносини між суб'єктом та об'єктом управління національною безпекою на основі чинних Конституції України, законів України, постанов Кабінету Міністрів України. Вони законодавчо визначають як засади так і компетенцію, права й обов'язки структурних підрозділів та посадових осіб суб'єктів управління, їхню підпорядкованість і спрямовані на забезпечення функціонування всіх ланок управління у сфері національної безпеки, успішне виконання покладених на суб'єкти забезпечення національної безпеки завдань і функцій. Авторами проілюстровано, як право сприяє забезпеченню управління національною безпекою в умовах державотворення в Україні, створює загальну нормативну систему, що впливає на формування управлінських рішень, і регулює економічні та фінансові відносини у суспільстві, що зумовлює ефективну управлінську безпеку та розвиває безпекознавство. Окрім цього, праву належить важливе місце в організації самої системи управління. Воно застосовується не тільки для регулювання суспільних відносин, але й у безпосередній організації управління. Ця організаційна функція права має істотне значення для всієї системи державного управління. Норми визначають, на якому рівні приймаються рішення, який порядок їхньої підготовки та реалізації, чиї рішення та для кого обов'язкові, як погоджуються управлінські рішення різних рівнів, яким чином здійснюється контроль за їхнім виконанням. Можливості права як засобу управління мають сприяти усвідомленню наявних протиріч, їхньому вирішенню, недопущенню трансформації у конфлікт, що є одним з найважливіших аспектів соціальної цінності права. На всіх стадіях процесу правотворчості мають розкриватися вимоги об'єктивних законів розвитку, зокрема й протиріччя в суспільних відносинах, що вимагають правового урегулювання.

Наші *прогнози на майбутнє* досить обнадійливі і оптимістичні. Адже попередній розвиток України свідчить, що на зламі кожної суспільно-політичної формації важко уникнути складнощів та потрясінь, яких не оминати стороною. А потім, із урахуванням як позитивного так і негативного досвіду управління безпековою сферою, якого нам не займати, встановлюється в державі мир і порядок. Як свідчать результати дослідження, найбільш небезпечною загрозою для України та її національної безпеки в сьогоденні умовах є владна корупція, яка разом із політичною складають системну корупцію. Сьогодні першочерговим є вдосконалення законодавства, що регулює діяльність політичних партій, законодавчої та виконавчої гілок влади, посилення відповідальності екстремістських елементів за вчинені кримінальні злочини. Слід здійснити практичні кроки щодо імплементації до національного законодавства положення статті 20 ратифікованої Україною Конвенції Організації Об'єднаних Націй проти корупції щодо відповідальності за незаконне збагачення.

### Використана література

1. Про національну безпеку України: Закон України від 21.06.18 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241.
2. Національна безпека: навчальний посібник / М.М. Чеховська, В.В. Остроухов, О.Л. Лісовська, І.М. Ничитайло, М.М. Присяжнюк, О.Ю. Полтораков, О.В. Чабала, В.С. Андрійчук, Н.В. Крапівіна; під заг. ред. проф. М.М. Чеховської. Київ: Нац. акад. СБ України, 2017. 344 с.
3. Foreign Policy. Spring, 1999. P. 104.
4. Стрельбицька Л.М., Стрельбицький М.П. Інформаційна безпека у сфері державного управління. *Юридичний вісник України*. 2010. № 37(793). С. 6-7.

5. Лисенко О.О. Правові аспекти захисту суспільства від негативного інформаційного впливу. *Інформаційна безпека людини, суспільства, держави*. 2010. № 2(4). С. 31-34.
6. Мороз В.В. Національна безпека – безпека людини. Київ: “Екслібрус”, 1994. 61 с.
7. Данільян О.Г., Дзьобань О.П., Панов М.І. Національна безпека України: структура та напрямки реалізації: навч. посіб. Харків: Фоліо, 2002. 285 с.
8. Битяк Ю.П. Адміністративне право України: підруч. Київ: Юрінком Інтер, 2005.
9. Гончаренко О., Джангужин Р., Лисицин Е. Громадський контроль і система національної безпеки. *Дзеркало тижня*. 2002. № 35. С. 1-12.
10. Організаційно-правові засади державного управління у галузі національної безпеки URL: <http://studies.in.ua/admin-pravo-shpora/2101-organizacyno-pravov-zasadi-derzhavnogo-upravlnnya-u-galuz-oboroni.html>
11. Нижник Н.Р., Мосов С.П. Концептуальний підхід до управлінської безпеки в системі державного управління в Україні. *Університетські наукові записки*. 2012. № 2 (42). С. 44-50.

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


УДК 343.3/.7:004.056 (477)

БАТИРГАРЕЄВА В.С., доктор юридичних наук, старший науковий співробітник,
головний науковий співробітник НДІ інформатики і права
НАПрН України, директор НДІ ВПЗ ім. академіка В.В. Сташиса
НАПрН України

ОСНОВНІ НАПРЯМИ ПРОТИДІЇ ПОШИРЕННЮ ДЕЗІНФОРМАЦІЇ (НА ПРИКЛАДІ ПАНДЕМІЇ COVID-19)

Анотація. У статті на прикладі гуманітарної кризи світового масштабу, пов'язаної із пандемією CoVID-19, представлені основні напрями протидії поширенню дезінформації, яка нерідко створює загрозу національній безпеці держав. До таких напрямів віднесено організаційно-інституційний, правовий та просвітницько-виховний.

Ключові слова: інформаційний простір, дезінформація, пандемія CoVID-19, інфодемія, кібербезпека.

Summary. The article uses the example of the global humanitarian crisis related to the CoVID-19 pandemic to present the main directions for counteracting the spread of misinformation, which often poses a threat to the national security of states. Such directions include organizational and institutional, legal and educational.

Keywords: information space, misinformation, CoVID-19 pandemic, infodemia, cybersecurity.

Аннотация. В статье на примере гуманитарного кризиса мирового масштаба, связанного с пандемией CoVID-19, представлены основные направления противодействия распространению дезинформации, которая нередко создает угрозу национальной безопасности государств. К таким направлениям отнесены организационно-институциональное, правовое и просветительско-воспитательное.

Ключевые слова: информационное пространство, дезинформация, пандемия CoVID-19, инфодемия, кибербезопасность.

Постановка проблеми. Чисельні проблеми людства, що, з одного боку, стали наслідком процесів глобалізації сучасного світу, а з другого – виявилися умовою пришвидшення настання ери цієї глобалізації, посилили дію такого потужного та часто непередбачуваного побічного ефекту, визначення якому “дезінформація”. Зазначений феномен, як небезпечний для соціального організму вірус, здатний в геометричній прогресії за нетривалий час поширюватися в інформаційному просторі, паразитуючи насамперед на болісних проблемах світу в цілому, окремих регіонів і країн. Останнім часом завдання адекватної рефлексії світової спільноти на будь-які випадки дезінформації, фреймом для яких якраз і стає глобалізаційна картина сучасного соціуму, поєднується із необхідністю вирішення проблеми приборкання пандемії CoVID-19. Такий тандем дезінформації та пандемії, окрім іншого, відтепер має братися до уваги у розробці будь-якого сценарію розвитку економічних, політичних та кримінальних реалій як національного, так і планетарного масштабів. Зазначені явища у своїй сукупності виявилися свого роду невідомими перемінними глобального характеру, що несподівано вплинули, у тому числі, й на визначення вектору прогностичних розрахунків майбутнього кількісно-якісного стану злочинності (принаймні на найближчу перспективу) та розробку стратегій запобігання їй. Разом із тим небезпека такого тандему полягає і в тому, що за принципом дії ланцюгової реакції дезінформація вже у теперішній час призводить до нового рівня ескалації напруження ситуації – інфодемії, яку можна охарактеризувати як масовий психоз в умовах глобалізації, коли навіть

незначний інформаційний поштовх (тим більше підкріплений відверто неправдивим контекстом) стосовно ключової у конкретний момент проблеми здатний за короткий час зруйнувати весь світопорядок, що вже встиг перетворитися на подібність глобального соціального організму, до того ж ураженого чисельними соціально-економічними, військово-політичними та соціоморальними хворобами.

Для того щоб історія людства в умовах чисельних викликів і загроз XXI ст., в оркестровці яких провідна партія сьогодні належить пандемо-інфодемії CoVID-19, не перетворилася остаточно на соціальний “титанік”, треба звернутися до аналізу сутності явища дезінформації та логіки множення небезпеки інфодемічного хаосу, у першу чергу, за допомогою сучасних технологічних можливостей інформаційного простору. Це необхідно так само й для того, щоб розробити ефективні заходи протидії цьому лиху, якими, зокрема, є й юридична відповідальність за дії, пов’язані з навмисним поширенням дезінформації.

Результати аналізу наукових публікацій. Аналізуючи природу поширення дезінформації, особливо в умовах так званої гуманітарної кризи, яка сьогодні зумовлена пандемією CoVID-19 та її наслідками, не можна не спиратися на той фундамент знань, що був зведений під час дослідження закономірностей функціонування та розвитку інформаційного простору як такого. При цьому неабиякий інтерес представниками різних дисциплінарних площин приділяється тим загрозам, що супроводжують практично неконтрольований процес нарощування потужностей медіапростору та викликають необхідність розробки заходів кібербезпеки. Отже, у цій сфері до основних дослідницьких дискурсів можна віднести: загальні питання діджиталізації суспільства та сфери права, зокрема [1 – 4]; шляхи зниження ризиків від інформаційного вандалізму, криміналу та тероризму [5; 6]; віктимізацію користувачів Інтернет-простору та питання інформаційної грамотності і гігієни [7; 8]; необхідність глобального реагування на кіберзлочинність [9 – 12]; аналіз природи та встановлення відмінності між явищами, що позначаються англійською як *misinformation* та *disinformation* [13; 14]; способи і швидкість поширення дезінформації у соціальних мережах та вимір довіри до джерел повідомлень [15; 16]; інформаційне протистояння великих соціальних груп та публічну дипломатію [17; 18]; тощо. Окремо слід наголосити на дослідженнях, присвячених стану злочинності та появі нових правопорушень, що з’являються саме під час гуманітарних криз [19 – 23]. Водночас ситуація, пов’язана із запровадженням карантинних заходів і суворих обмежень у зв’язку з пандемією CoVID-19, підштовхує людство зайвий раз замислитися над характером і масштабами тієї шкоди, яку здатна завдати дезінформація, породжена будь-якою гуманітарною кризою чи то світового рівня, чи то навіть локального характеру. У цій ситуації невідкладно має наставати певна реакція, образно кажучи, інформаційних фільтрів, які активізуються зацікавленими учасниками медіапростору з тим, щоб ефективно протидіяти дезінформаційним джерелам.

Метою статті є підсумок аналізу небезпеки інфодемічного хаосу, який створюється внаслідок процвітання явища дезінформації, та, спираючись на міжнародний і національний досвід, ініціативи та пропозиції, окреслення векторів можливої протидії дезінформації, які здатні скоротити масштаби ураженості суспільства неправдивою інформацією, що може привести сьогодні до розлогої палітри вкрай непередбачуваних наслідків.

Виклад основного матеріалу. Для України створення системи надійного захисту від будь-яких дезінформаційних потоків уявляється важливим у зв’язку з обранням нашою державою курсу на інтеграцію з Європейським Союзом, засадою існування якого

є, у тому числі, й невід’ємне право людини на отримання достовірної інформації. Створення такої системи стає дуже важливим в умовах, коли дезінформація про коронавірус заповнила інформаційний простір, особливо соціальні мережі Інтернету, що є головними комунікаторами для користувачів всесвітньої павутини.

У законодавстві України немає чіткого визначення явищу дезінформації та фактично не передбачено серйозних правових наслідків за її поширення, навіть незважаючи на наявність чисельних гуманітарних криз, які зачіпають нашу країну, та положення Доктрини інформаційної безпеки України, затвердженої Указом Президента України від 25 лютого 2017 р. № 47/2017, про боротьбу з дезінформацією та деструктивною пропагандою з боку Російської Федерації як один із пріоритетів державної політики в інформаційній сфері. Тобто навіть перебуваючи у стані надання відсічі та стримування збройної агресії на Сході нашої країни, визнаючи необхідність проведення нагальних реформ у безпековій сфері, а до того ж й переживаючи тяжкі наслідки поширення небезпечного вірусу, у теперішній час фактично не можна ефективно протидіяти поширенню дезінформації.

Однак перш ніж визначитися з можливими напрямками протидії остигній (особливо в ситуації, в якій зараз перебуває Україна), треба чітко зрозуміти, що представляє собою феномен дезінформації, адже навіть визначення цього феномену набуває різного забарвлення у тих чи інших системах суспільно-політичного виміру. Так, якщо звернутися до енциклопедичної літератури, виданої за радянських часів, то можемо побачити, що під дезінформацією мали на увазі поширення спотворених або завідомо неправдивих відомостей для досягнення (у буржуазному суспільстві) військових (введення противника в оману) або інших цілей [24, с. 372]. Ближче до істинного змісту розглядуваного явища є, напевно, таке його визначення: дезінформація – завідомо неправдива інформація, що надається противнику або діловому партнеру для більш ефективного ведення бойових дій, співпраці, перевірки на витік інформації і напрямку її витоку, виявлення потенційних клієнтів “чорного ринку” тощо [25]. Проте і це визначення, на наш погляд, є неповним. Адже за його межами залишаються, власне, процес впливу за допомогою неправдивої інформації на свідомість окремих осіб, великих груп осіб або навіть населення країни, регіону, світу, а так само результати подібного впливу. Причому, якими б не були неправдиві відомості, способи та засоби їх поширення, а також цільова аудиторія впливу, однак мета, яку переслідує “генератор” дезінформації, як правило, завжди одна, а саме: “мішень” має здійснити дії або відмовитися від їх вчинення саме у такий спосіб, як це вигідно, умовно кажучи, маніпулятору. Разом із цим побічним “ефектом” дезінформаційного впливу найчастіше виступає страх, обурення, злість, занепокоєння, засмучення, дезорієнтація, фрустрація та ін. Звісно ж, своєю поведінкою, зумовленою впливом дезінформації, суб’єкти, на які спрямована остання, лише погіршують певну ситуацію, свій власний стан, вдаючись до помилкових дій та приймаючи неправильні рішення.

Таким чином, все це може мати вельми негативні і навіть тяжкі наслідки для окремої особи, суспільства, держави чи держав. При цьому можна зазначити про достатньо різні види дезінформації, починаючи від відвертого підбурювання до насильства, геноциду та поширення неправдивої інформації, покликаної зачепити націоналістичні струнки в душах людей, і закінчуючи навмисним спотворенням інформації для формування громадської думки [26]. З останнім проявом дезінформації у теперішній час ми особливо часто маємо справу. Це зумовлено тим, що після спалаху коронавірусної хвороби наприкінці 2019 р. і ще до часу офіційної об’яви у світі пандемії, в Інтернеті, різного роду соціальних мережах і месенджерах стали

поширюватися неправдиві повідомлення про походження, масштаби поширення, профілактику, лікування та різні інші аспекти захворювання внаслідок інфікування цим вірусом. Також набули популярності так звані конспірологічні теорії змови та висловлювання ненависті. Як підкреслюють зарубіжні фахівці K. Usher, J. Durkin та N. Bhullar, тривога і страх, пов'язані з інфекцією, можуть призвести до актів дискримінації [27, с. 315]. Наприклад, S.-Y. Ren *et al.* відзначають, що мешканці Ухані зазнають нападів із боку інших китайців і звинувачуються в спалаху CoVID-19; китайці з тих пір піддаються міжнародній стигматизації [28]. Свого часу, за свідченням S. Monson, спалах лихоманки Ебола в 2014 р., що вважався проблемою африканського походження, призвів до дискримінації осіб африканського походження [29]. До речі, об'єктом стигматизації і дискримінації можуть виявитися й конкретні люди, які заразилися хворобою. В Україні відомі випадки, коли домівки, в яких проживають інфіковані або навіть особи з підозрою на інфекцію, помічалися так званими “інформаційними листівками” [30]. І одразу ж на проросійських сайтах з'явилися повідомлення про те, що вже на сотнях домівок в Україні наклеєні відповідні “мітки”^{*}. І таких прикладів, на жаль, чимало.

Отже, на прикладі ситуації із коронавірусом спробуємо систематизувати можливі заходи протидії поширенню відповідної дезінформації, які, на наш погляд, доцільно брати у подальшому за основу під час розробки дієвих стратегій запобігання фактам поширення будь-якої дезінформації у нашій країні.

Перший напрям протидії поширенню дезінформації назвемо організаційно-інституційним. Його сутність полягає в тому, що зацікавлені учасники медіапростору активно вживають спеціальних заходів щодо спростування дезінформації та убезпечення від неї на майбутнє. Як правило, цим займаються як офіційні структури різного рівня, форми та призначення (міжнародні, національні, регіональні та ін.) та їх представники, так й окремі неформальні учасники (інституції) медіапростору, інформаційна репутація яких серед користувачів відповідних інформаційних ресурсів є високою. Наприклад, найбільші технологічні компанії Facebook, Google і Microsoft, а також LinkedIn, Reddit, Twitter і YouTube повідомили у спільній заяві, що вони взаємодіють з метою протидії шахрайству і дезінформації про новий тип коронавірусу, відсилаючи користувачів соціальних мереж, які коментували відповідні пости, ставили під ними лайк або ділилися цією інформацією з будь-яким, на сторінку “Руйнівники міфів” на сайті Всесвітньої організації охорони здоров'я [31]. До речі, згадані інтернет-платформи є учасниками так званого Кодексу поведінки проти дезінформації, започаткованого Єврокомісією у 2019 р., до якого запросили приєднуватися так само представників бізнесу, рекламні агенції та інших представників інформаційної галузі [32]. У свою чергу, чимало друкованих видань із платною підпискою на свої матеріали (наприклад, The New York Times, Bloomberg та ін.) відкрили вільний доступ до інформації щодо коронавірусу, розміщеної на їх офіційних сайтах [33; 34]. Водночас не слід відкидати й технічну можливість блокування роботи певних платформ, що використовуються для поширення дезінформації. Звісно ж, координально проблему у такий спосіб вирішити неможливо, однак за допомогою такого кроку вдасться забезпечити “утримання” розглядуваної проблеми на певному “допустимому” рівні, який не призведе до створення ситуації загрози національним інтересам держави та інтересам окремих громадян.

^{*} Від авт. З етичних та правових міркувань нами не наводяться посилання на ці сайти.

Вагома роль офіційних джерел якісної інформації також визначається й у спеціальній літературі. Так, наголошується, що проблему дезінформації, тривоги населення та чуток повинні вирішувати посадовці органів охорони здоров'я (Madhav *et al.* (2017)) [35, с. 328] та що моніторинг неофіційних джерел інформації, включаючи неправдиві відомості у вигляді чуток, є корисним особливо в тих регіонах, де прогалини в системі охорони здоров'я є значними (Samaan *et al.* (2005)) [36]. Свого часу, коли стався спалах пташиного грипу, Західно-Тихоокеанське регіональне бюро ВООЗ стало координаційним центром із виявлення дезінформації (чуток) і координації їх розслідувань у регіоні [36, с. 463].

Виконуючи функцію щодо неупередженого інформування громадськості з приводу криміногенної обстановки в європейському регіоні під час пандемії, така інституція, як Європол, попутно вносить свій внесок у розвінчання багатьох чуток, пов'язаних із протіканням хвороби. Нприклад, нещодавно Європол опублікував доповідь під назвою “Pandemic Profiteering: How Criminals Exploit the CoVID-19 Crisis” (“Пандемічний спекулянт: як злочинці експлуатують кризу CoVID-19”, березень 2020), в якій стисло викладено позицію аналітиків Європолу щодо головних змін у кримінальній дійсності пандемічного періоду. Зокрема, відзначається, що правопорушники швидко скористалися можливостями, які відкриває криза, адаптуючи до цього свою злочинну діяльність або вдаючись до вчинення нових злочинних дій. Чинниками, що впливають на зазначені зміни, зокрема, є: високий попит на певні товари, як-от: захисне спорядження та фармацевтична продукція; зниження мобільності і потоку людей до ЄС або транзитом через ЄС; залишення громадян дома та дистанційний характер роботи з використанням можливостей Інтернет-простору; непомітність деяких кримінальних дій та їх перенесення у домашні умови або на он-лайн-пристрої внаслідок обмежень у суспільному житті; вразливість людей через підвищення тривоги і страху; скорочення поставок певних незаконних товарів до ЄС [37]. При цьому, ґрунтуючись на інформації, наданій державами-членами ЄС та власними експертами, Європолом робиться висновок про зростання кіберзлочинності, шахрайства, продажу контрафактної медичної та санітарно-гігієнічної продукції, засобів індивідуального захисту та формування нового, так званого карантинного типу організованої злочинності, коли групи правопорушників реалізують цілі схеми, видаючи себе за представників органів влади та медиків із метою вчинення шахрайства і крадіжок [37]. Можна зробити висновок, що у підґрунті багатьох із перелічених злочинних трендів знаходиться таке фонове явище правопорушень, як дезінформація.

Так само у березні 2020 р. Європейська служба зовнішніх зв'язків (European External Action Service) підготувала Спеціальний звіт під назвою “Дезінформація про коронавірус – короткий огляд інформаційного середовища”, в якому робиться огляд найбільш поширених неправдивих наративів, на кшталт таких, що коронавірус – біологічна зброя певних країн; поширення інфекції походить із США; спалах хвороби викликаний мігрантами, що перебувають на території ЄС; CoVID-19 є наслідком розвитку 5G; Шенгенська зона припинила своє існування тощо. При цьому у зазначеному Звіті підкреслюється, що уряди та органи охорони здоров'я намагаються надавати достовірну інформацію про коронавірусну інфекцію CoVID-19, а соціальні мережі шукають ефективні способи просування цього контенту, одночасно видаляючи сумнівний контент або знижуючи його пріоритет [38].

Таким чином, моніторинг медіапростору та виявлення в ньому дезінформації має спрямовуватися: по-перше, на зниження потенціалу цього явища впливати на розум та емоції людей; по-друге, на посилення відповідної роботи з інформування громадськості

та посадових осіб про стан епідемічної ситуації в країні; по-третє, на сприяння швидкому реагуванню відповідних суб'єктів щодо випадків подібної неправдивої інформації та підвищення готовності своєчасно посилити заходи з охорони громадського здоров'я.

Другий напрям протидії поширенню дезінформації позначимо, як правовий. За справедливим зауваженням О.О. Костенко, “очевидно, сьогодні потребують вирішення проблеми реалізації кримінальної відповідальності за поширення такої дезінформації, яка може провокувати масові заворушення, громадянські конфлікти, паніку у суспільстві, деструктивні громадянські акції, міжнаціональну ворожнечу тощо” [39, с. 299]. Напевно, законодавчий рівень слід визнати як найбільш радикальний метод протидії поширенню дезінформації щодо ситуації із пандемією CoVID-19.

Щоб оцінити можливості цього напрямку, треба проаналізувати стан правового забезпечення протидії дезінформації на теперішній час. Звернемося, наприклад, до досвіду Сполучених Штатів Америки, де наприкінці 2016 р. приймається Закон про протидію іноземній пропаганді та дезінформації (Countering Foreign Propaganda and Disinformation Act) [40]. Одним із результатів прийняття зазначеного закону стало утворення Global Engagement Center (Центру глобальної взаємодії), метою якого визначено координацію дій уряду США щодо боротьби з пропагандою та дезінформацією іноземних держав і терористичних організацій. Сьогодні серед заходів цього Центру значиться й протидія конспірологічним версіям причин походження та поширення пандемії коронавірусу [41].

Цікаво навести й досвід деяких інших країн. Якщо звернутися до останніх подій у Китаї, то в цій країні в умовах поширення епідемії дезінформація в соціальних мережах була визнана кримінальним правопорушенням, про що на початку березня 2020 р. внесено відповідну поправку до кримінального закону [42, с. 4]. Аналогічний закон прийнято й в Індонезії. Строком ув'язнення на п'ять років або штрафом близько 800 дол. США може закінчитися публікація неперевіреної інформації про поширення коронавірусу у Саудівській Аравії [42, с. 4].

Так само кримінальна відповідальність за поширення такої дезінформації передбачено у низці країн постадянського простору. Наприклад, в Узбекистані особам, винним у поширенні неправдивої інформації, може загрожувати покарання у виді штрафу від 4,6 до 9,2 тис. дол. США, обов'язкові громадські роботи до 360 год., виправні роботи або навіть позбавлення волі строком до трьох років. У Молдові заборонено висловлювати власну думку про коронавірус під час різноманітних дебатів і ток-шоу, а тому мас-медіа зобов'язали давати тільки затверджену владою інформацію. За посилання на інформацію, взяту не з офіційних джерел, вірменським ЗМІ загрожує штраф у розмірі від 1016 до 1626 дол. США [42, с. 4]. Справедливості заради треба навести і спроби РФ боротися з поширенням завідомо неправдивої інформації, що, звісно ж, може стосуватися й ситуації, пов'язаної із пандемією CoVID-19. У квітні 2020 р. до КК РФ введено дві нові статті 207.1 “Публічне поширення завідомо неправдивої інформації про обставини, що становлять загрозу життю та безпеці громадян” та 207.2. “Публічне поширення завідомо неправдивої суспільно значущої інформації, що спричинило тяжкі наслідки” [43].

Завершити стислий огляд протидії поширенню дезінформації за допомогою правових засобів слід аналізом вітчизняної практики. На наш погляд, внаслідок відсутності у чинному законодавстві України відповідальності за систематичне умисне поширення дезінформації наразі назріла потреба у прийнятті законопроекту “Про протидію дезінформації”. Нещодавно такий документ був презентований Міністерством

культури, молоді та спорту України. Метою цього документа є захист інформаційного простору України від дезінформації та гібридних загроз із питань, які становлять суспільний інтерес і стосуються національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, довкілля тощо [44]. У проекті цього Закону України наводиться достатньо непогане визначення дезінформації, під якою слід розуміти недостовірну інформацію з питань, що становлять суспільний інтерес, зокрема стосовно національної безпеки, територіальної цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, стану довкілля [44]. Із цього визначення можна зробити висновок, що не будь-які неправдиві відомості можуть набувати "статусу" дезінформації, а лише ті, що зачіпають основи національної безпеки, базові права народу та окремих осіб, придатність довкілля бути безпечним для людини та всього живого. Як правило, дезінформація вирізняється якістю "масовості", тобто вона є доступною для необмеженого (фактично невизначеного) кола осіб. І будь-яка особа має можливість отримати доступ до неї у будь-який час та з будь-якого місця.

Повторимося, але факти дезінформації сьогодні знаходяться нібито над законом, адже чинне законодавство України не передбачає навіть можливості звернутися будь-кому до суду з приводу поширення такої неправдивої інформації. Іншими словами, немає ані відповідної нормативної бази, ані механізму захисту будь-кого від неї. Це, власне, й спонукає замислитися над проблемою захисту від дезінформації.

У проекті зазначеного вище Закону України пропонується встановити адміністративну відповідальність за поширення дезінформації, порушення правил спростування, надання відповіді та вимог прозорості, а так само встановити кримінальну відповідальність за системне та умисне масове поширення дезінформації. Що стосується кримінальної відповідальності, то розробниками законопроекту запропоновано за систематичне умисне масове розповсюдження завідомо недостовірних повідомлень про факти, події або явища, що становить загрозу національній безпеці, громадській безпеці, територіальній цілісності, суверенітету, обороноздатності України, права українського народу на самовизначення, життя та здоров'я громадян, стану довкілля у період відсутності повного контролю України за її державним кордоном карати штрафом від 5 тисяч до 10 тисяч неоподаткованих мінімумів доходів громадян або виправними роботами від 1 до 2 років. Разом із цим передбачено і низку кваліфікуючих та особливо кваліфікуючих обставин, серед яких: систематичне умисне масове розповсюдження дезінформації з використанням комп'ютерних програм, призначених для автоматичного масового розповсюдження інформації (ботів), спеціально організованої системи (групи) облікових записів або користувачів інформаційних послуг, засобів умисного фальшування (підробки) джерел інформації, фінансування подібних дій та вчинення таких лій повторно або у складі організованої злочинної групи, настання тяжких наслідків чи спричинення матеріальної шкоди у великому розмірі [44].

Можливо, якість законодавчої техніки та багатьох положень й викликає серйозні зауваження, проте це перший крок на шляху протидії суспільно небезпечному явищу, яким сьогодні, безумовно, є дезінформації в умовах пандемії CoVID-19. Проте одними лише кримінально-правовими засобами здолати це явище не уявляється можливим, тому необхідним уявляється й дослідження феномену дезінформації та її різновидів із позиції кримінологічної доктрини.

Нарешті, ще одним важливим напрямом протидії поширенню дезінформації із приводу пандемії CoVID-19 є виховна та просвітницька діяльність. Чимало експертів в галузі боротьби із дезінформацією закликають користувачів Інтернет-простору дотримуватися так званої інформаційної гігієни, надаючи пораду – звертатися насамперед лише до перевірених професійних акаунтів новинних, урядових і відомих громадських організацій, оскільки доступ до неофіційної інформації може сприяти подальшому, часто непотрібному неспокою та паніці [45]. Водночас не можна не зазначити, що розвиток медіаграмотності є вельми тривалим процесом, пов'язаним із доланням “рефлексу Земмельвейса” [46], сутність якого полягає в тому, що люди бажають вірити перш за все тим фактам, які їм з якихось причин подобаються. До того ж щоб змінити ставлення людей до певної інформації, сформувати відповідні навички розпізнавати недоброякісну інформацію та критично ставитися до неї, напевно, потрібні значний час та наполеглива просвітницька робота в цьому напрямку. Тому роботу з підвищення загальної медіаграмотності треба починати ще з дитинства, оскільки можливості медіапростору сьогодні є інструментом комунікації навіть у дітей дошкільного віку. Логічно постає запитання: хто повинен проводити подібну роботу? На наш погляд, відповідними суб'єктами у цьому разі мають стати представники технологічних компаній (Facebook, Google, Microsoft, You Tube та ін.), провайдери, ЗМІ, зокрема електронні, спеціалізовані організації, що викривають дезінформацію, інформаційні волонтери, блогери, педагоги, представники органів влади та багато інших інституцій сучасної комунікації. При цьому особлива роль має відводитися саме блогерам, адже, як зазначають фахівці, “часто люди довіряють більше блогерам, ніж традиційним джерелам інформації. Враховуючи цей ступінь довіри, лідери думок здатні спільно зупиняти хвилі дезінформації та чуток” [47]. У такій ситуації люди (особливо в ситуаціях, подібних тій, в якій зараз перебуває світ) мають взяти за правило – шукати кілька інформаційних джерел (ЗМІ, перевірени акаунти у соціальних мережах, що існують вже тривалий час, офіційні сайти тощо), приділяючи пильну увагу тому контексту, який публікує той чи інший ресурс, та не поширюючи певний контекст, якщо існують сумніви у правдивості його змісту.

Висновки.

Дезінформація (особливо в умовах існування так званих невідомих змінних глобального характеру, якою сьогодні якраз і виступає пандемія коронавірусу) перетворюється на проблему національної безпеки, що здатна дестабілізувати світовий уклад. Оскільки дезінформація з приводу пандемії CoVID-19 та її наслідків здатна ще більше посилити потенційну загрозу суспільній стабільності в цілому, а так само життю та здоров'ю громадян, тому цей феномен слід розглядати саме у контексті безпекового виміру сучасного світу, вважаючи його одним із найпомітніших викликів, що супроводжує останнім часом процес глобалізації буття будь-якого суб'єкта інформаційних відносин.

Коефіцієнт корисної дії від боротьби з дезінформацією щодо ситуації з коронавірусом, безумовно, підвищуватиметься, якщо ця діяльність сфокусована за кількома стратегічними напрямками. Ефективними заходами, що не вимагають будь-яких часових затрат та поєднуються в окремий самостійний напрям, є заходи, пов'язані зі спростуванням відповідної дезінформації та убезпеченням у такий спосіб медіапростору від неї на майбутнє. Ще одним напрямом протидії поширенню дезінформації є законодавчий рівень. Для розв'язання аналізованої проблеми з огляду на можливості зазначеного напрямку якомога скоріше необхідно розпочати, з одного боку, формування міжнародного законодавства, спрямованого на рішучу боротьбу з фейковими новинами,

а з другого боку, на національному рівні слід опрацювати законодавчі механізми юридичної відповідальності, спрямовані на недопущення генерування або ретрансляції подібних новин принаймні за участю учасників інформаційного простору, внаслідок чого створюється загроза національній безпеці нашої держави. У свою чергу, метою медіавиховання та медіапросвітництва є формування у людини критичного стилю мислення стосовно наявної інформації у необмеженому просторі новин.

Використана література

1. Valeev D.K., Nuriev A. G. Digitization of Law: Some Problematic Aspects. *Journal of Politics and Law*. 2019. Vol. 12, No. 5. P. 135-139.
2. Baker M. Digital Transformation. Create Space Independent Publishing Platform, 2014, 226 p.
3. Батиргарєєва В.С. До питання ризиків та загроз, пов'язаних із діджиталізацією України: зб. тез доповідей учасників Всеукраїнської науково-практичної Інтернет-конференції *Актуальні проблеми інформаційного права в умовах глобалізації*, м. Черкаси, 28 лист. 2019 року. Черкаси: Східноєвропейський університет економіки і менеджменту, 2019. С. 79-81.
4. Григорьев В.Н., Суходолов А.П., Ованесян С.С., Спасенникова М.Г., Тюньков В.В. Цифровые информационные платформы как предмет нормативно-правового регулирования в сфере уголовного судопроизводства. *Всероссийский криминологический журнал*. 2019. Т. 13. № 6. С. 873-883.
5. Осипов В.Ю., Юсупов Р.М. Информационный вандализм, криминал и терроризм как современные угрозы обществу. Тр. СПИИРАН. 2009. Вып. 8. С. 34-45.
6. Албул С.В. Протидія інформаційним загрозам в умовах антитерористичної операції: матеріали Всеукраїнської науково-практичної *Кібербезпека в Україні: правові та організаційні питання*. Одеса: ОДУВС, 2016. С. 7-8.
7. Levy K., Schneier B. Privacy Threats in Intimate Relationships. *Journal of Cybersecurity*. Vol. 6. Issue 1. 2020. URL: <https://academic.oup.com/cybersecurity/article/6/1/tyaa006/5849222?searchresult=1> (дата звернення: 02.06.2020).
8. Java S., Basheer F. L., Riaz S., Kaur M. J., Mushtaq A. Detection of Online Manipulation to Prevent Users Victimization. *Amity International Conference on Artificial Intelligence (AICAI)* (Dubai, United Arab Emirates 4-6 February 2019). Dubai: Amity University Dubai, 2019. P. 593-599.
9. Tabassum A., Mustafa M. S., Maadeed S. A. A. The need for a global response against cybercrime: Qatar as a case study. *6th International Symposium on Digital Forensic and Security (ISDFS)*. (Antalya, Turkey, Mar 22, 2018 – Mar 25, 2018) Antalya: IEEE, 2018. P. 1-6.
10. Александров А.С., Александрова И.А. Организационно-правовой механизм противодействия киберпреступности в эпоху цифровых технологий. *Юридическая наука и практика на рубеже эпох: уроки прошлого, взгляд в будущее*: сб. тр. / отв. ред. Г.Г. Бриль, В.В. Груздев. Кострома, 2018. С. 303-309.
11. Лефтеров Л.В. Криминологическая характеристика мошенничества, совершенного с использованием электронно-вычислительной техники. *Leges i viae*. 2018. № 8-2. С. 69-73.
12. Котенко И.В., Юсупов Р.М. Информационные технологии для борьбы с терроризмом. *Защита информации. ИНСАЙД*. 2009. № 2 (26). С. 74-79.
13. Fox C.J. Information and Misinformation. In book: *An Investigation of the Notions of Information, Misinformation, Informing and Misinforming*. Westport Conn: Greenwood press, 1983. 223 с.
14. Botha J., Pieterse H. Fake News and Deepfakes. *A Dangerous Threat for 21st Century Information Security*: 15th International Conference on Cyber Warfare and Security: Conference Paper. Norfolk, USA, 2020. P. 57-66.
15. Buchanan T., Benson V.B. Spreading disinformation on Facebook: Do trust in message source, risk propensity or personality affect the organic reach of 'fake news'? *Social Media and Society*. 2019. 5 (4). P. 1-9.

16. Zubiaga A., Aker A., Bontcheva K., Liakata M., Procter R. Detection and Resolution of Rumours in Social Media: A Survey. *ACM Computing Surveys*. 51(2). February 2018. Article No. 32. URL: <https://doi.org/10.1145/3161603> (дата звернення: 20.06.2020).
17. Golovchenko Ye., Hartmann M., Adler-Nissen R. State, Media and Civil Society in the Information Warfare over Ukraine. *International Affairs*. 2018. Vol. 95. Issue 5. P. 975-994.
18. Lewandowsky S., Stritzke W.G.K., Freund A.M., Oberauer K., Krueger J.I. Misinformation, Disinformation and Violent Conflict: From Iraq and the “War on Terror” to Future Threats to Peace. *American Psychologist*. 2013. 68 (7). P. 487–501.
19. Tran T., Valecha R., Rad P., Rao R. An Investigation of Misinformation Harms Related to Social Media During Humanitarian Crises. *Secure Knowledge Management In Artificial Intelligence Era: 8th International Conference (Goa, India, December 21-22, 2019)*. India: SKM, 2019. P. 167-181.
20. Батиргарєєва В.С. Світ ніколи не буде таким, як раніше: до картини кримінологічного футуризму: матеріали Інтернет-конференції *Правові засади епідемічної безпеки: виклики та перспективи*, м. Полтава, 29 квіт. 2020 р. Харків: Право, 2020. С. 26-30.
21. Гуторова Н.О. Протидія фальсифікації медичних виробів в період пандемії COVID-19: матеріали Інтернет-конференції *Правові засади епідемічної безпеки: виклики та перспективи*, м. Полтава, 29 квіт. 2020 р. Харків: Право, 2020. С. 73-75.
22. Калініна А.В. Карантин в Україні та фонові для злочинності явища. *Правові засади епідемічної безпеки: виклики та перспективи: матеріали Інтернет-конференції*, м. Полтава, 29 квіт. 2020 р. Харків: Право, 2020. С. 129-131.
23. Колодяжний М. Г. Вплив карантину на стан злочинності в Україні: матеріали Інтернет-конференції *Правові засади епідемічної безпеки: виклики та перспективи*, м. Полтава, 29 квіт. 2020 р. Харків: Право, 2020. С. 160-153.
24. Советский энциклопедический словарь. Москва: Советская энциклопедия. 1979. 1600 с.
25. Дезинформация. URL: <https://dic.academic.ru/dic.nsf/ruwiki/1297893> (дата звернення: 21.06.2020).
26. Что такое дезинформация? Описание и определение термина. URL: <https://biznes-prost.ru/dezinformaciya.html> (дата звернення: 19.06.2020).
27. Usher K., Durkin J., Bhullar N. The COVID-19 pandemic and mental health impacts. *International Journal of Mental Health Nursing*. 2020. No 29. P. 315-318.
28. Ren S.-Y., Gao R.-D., Chen Y.-L. (2020). Fear Can Be More Harmful than the Severe Acute Respiratory Syndrome Coronavirus 2 in Controlling the Coronavirus Disease 2019 Epidemic. *World Journal of Clinical Cases*. 2020. Feb 26. Vol. 8 (4). P. 652-657.
29. Monson S. Ebola as African: American Media Discourses of Panic and Otherization. *Africa Today*. 2017. Vol. 63 (3). P. 3-27.
30. Нечет Т.В. Днепре дома с потенциально больными коронавирусом стали помечать листовками. URL: <https://kp.ua/covid/666307-v-dnepre-doma-s-potentsyalno-bolnomy-koronavirus-om-staly-pomechat-lystovkam> (дата звернення: 15.06.2020).
31. В Facebook придумали новый способ борьбы с фейками о коронавирусе. URL: <https://tech.liga.net/technology/novosti/v-facebook-pridumali-novyuy-sposob-borby-s-feykami-o-korona-viruse> (дата звернення: 19.06.2020).
32. Єврокомісія презентувала Кодекс протидії фейкам. URL: <https://www.ukrinform.ua/rubric-world/2629474-evrokomisia-prezentovala-kodeks-protidii-fejkam.html> (дата звернення: 20.06.2020).
33. The Coronavirus Outbreak. URL: <https://www.nytimes.com/news-event/coronavirus> (дата звернення: 16.06.2020).
34. Major Publishers Take Down Paywalls for Coronavirus Coverage. URL: <https://www.adweek.com/digital/major-publishers-take-down-paywalls-for-coronavirus-coverage> (дата звернення: 20.06.2020).
35. Madhav N., Oppenheim B., Gallivan M., Mulembakani P., Rubin E. et. al. Pandemics: Risks, Impacts, and Mitigation. In: *Disease Control Priorities: Improving Health and Reducing Poverty*

(third edition): Vol. 9, edited by D. T. Jamison, H. Gelband, S. Horton, P. Jha, R. Laxminarayan, C.N. Mock, R. Nugent. Washington, DC: World Bank Group, 2018. P. 315-345.

36. Samaan G., Patel M., Olowokure B., Roces M. C., Oshitani H. et al. Rumor Surveillance and Avian Influenza H5N1. *Emerging Infectious Diseases*. 2005. Vol. 11 (No 3). P. 463-466.

37. Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis. URL: <https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis> (дата звернення: 21.06.2020).

38. Специальный отчет Европейской службы внешних связей (ЕСВС): Дезинформация о коронавирусе – краткий обзор информационной среды. URL: <https://euvsdisinfo.eu/ru> (дата звернення: 21.06.2020).

39. Костенко О.О. Щодо відповідальності за поширення суспільно небезпечної дезінформації (дискусійні питання). *Альманах права. Право і прогрес: складові забезпечення в сучасних умовах*. Вип. 7. Київ: Ін-т держави і права ім. В. М. Корецького НАН України, 2016. С. 296-300.

40. Countering Foreign Propaganda and Disinformation Act. December, 8. 2016. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/3274/text> (дата звернення: 17.06. 2020).

41. Coronavirus: Russia denies spreading US conspiracy on social media. URL: <https://www.bbc.com/news/world-us-canada-51599009> (дата звернення: 14.06.2020).

42. Коваленко М., Беленькая М., Тарасенко П. Вакцина от фейков. Как мир борется с дезинформацией о пандемии. Газета “Коммерсантъ”. 2020. 31 марта. № 57. С. 4.

43. О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный Закон от 01.04.20 г. № 100-ФЗ. *Российская газета*. № 72. 2020. 3 апр.

44. Про протидію дезінформації: презентація законопроекту. URL: <https://mkms.gov.ua/files/InformPolityka.pdf> (дата звернення: 30.05.2020).

45. Johal Sarbjit S. Psychosocial Impacts of Quarantine During Disease Outbreaks and Interventions that May Help to Relieve Strain. *New Zealand Medical Journal*. 2009. June, 5. Vol. 122 (1296). P. 47-52.

46. Gupta V. K., Saini C., Oberoi M., Kalra G., Nasir M. I. Semmelweis Reflex: An Age-Old Prejudice. *World Neurosurgery*. 2020. April. No. 136. P. 119-125.

47. Кіщак В. Недовіра, хаос та паніка. Як дезінформація впливає на людей і що з цим робити. URL: https://espresso.tv/article/2020/04/23/nedovira_khaos_ta_panika_yak_dezinformaciya_vplyvaye_na_lyudey_i_scho_z_cym_robity (дата звернення: 18.06.2020).

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

УДК 659.3:351:864 (477.6)

**МАЄВСЬКИЙ О.О.**, кандидат історичних наук, старший науковий співробітник  
відділу історії України періоду Другої світової війни  
Інституту історії України НАН України.  
ORCID: <https://orcid.org/0000-0001-9926-3270>.

## ФОРМУВАННЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ В ТАК ЗВАНИХ “ДНР” ТА “ЛНР” МЕТОДАМИ ЕКСПЛУАТАЦІЇ ВІЗУАЛЬНИХ ОБРАЗІВ ДРУГОЇ СВІТОВОЇ ВІЙНИ

**Анотація.** У статті аналізуються інформаційно-психологічні кампанії, які проводяться ідеологами “русского мира” на тимчасово окупованій території України. Визначені основні акценти, методи та підходи, якими послуговуються пропагандисти під час проведення маніпулятивних акцій. Проаналізовано візуальне наповнення агітаційно-пропагандистської продукції під час проведення масових публічних заходів. Окреслена цільова аудиторія аудіо-візуальної продукції, а також основні сюжетні лінії й походження сценарних планів для проведення масових урочистих заходів, пов’язаних з культурою пам’яті про Другу світову війну. Виявлено спільні та відмінні риси проведених урочистостей у Російській Федерації та у так званих “ДНР” та “ЛНР”. Проаналізовано проросійський ідеологічний вплив на гуманітарну та соціальну політику, а особливо на політику пам’яті.

**Ключові слова:** інформаційне поле, пропаганда, агітація, навіювання, компрометація, маніпуляція, інформаційні потоки, морально-психологічний стан, День перемоги, інформаційний простір, Друга світова війна, фейк, “ДНР”, “ЛНР”.

**Summary.** The article analyzes information and psychological campaigns conducted by ideologists of the “Russian world” in the temporarily occupied territory of Ukraine. The main accents, methods and approaches used by propagandists during the conduct of manipulative actions are identified. The visual filling of propaganda products during mass public events is analyzed. The target audience of audio-visual products is outlined, as well as the main storylines and the origin of the scripts for holding mass celebrations related to the memory of the Second world war. The common and distinctive features of the celebrations in the Russian Federation and in the so-called “DNR” and “LPR” were revealed. The pro-Russian ideological influence on humanitarian and social policy, and especially on memory policy, is analyzed.

**Keywords:** information field, propaganda, agitation, suggestion, compromise, manipulation, information flows, moral and psychological state, Victory Day, information space, WWII, fake, “DNR”, “LPR”.

**Аннотация.** В статье анализируются информационно-психологические кампании, которые проводятся идеологами “русского мира” на временно оккупированной территории Украины. Определены основные акценты, методы и подходы, которыми пользуются пропагандисты во время проведения манипулятивных акций. Проанализировано визуальное наполнение агитационно-пропагандистской продукции во время проведения массовых публичных мероприятий. Обозначенная целевая аудитория аудиовизуальной продукции, а также основные сюжетные линии и происхождение сценарных планов для проведения массовых торжественных мероприятий, связанных с культурой памяти о Второй мировой войне. Выявлены общие и отличительные черты проведенных торжеств в Российской Федерации и в так называемых “ДНР” и “ЛНР”. Проанализировано пророссийское идеологическое воздействие на гуманитарную и социальную политику, в особенности на политику памяти.

**Ключевые слова:** *информационное поле, пропаганда, агитация, внушение, компрометация, манипуляция, информационные потоки, морально-психологическое состояние, День победы, информационное пространство, Вторая мировая война, фейк, “ДНР”, “ЛНР”.*

**Постановка проблеми.** На тимчасово окупованій території України ворог розгорнув широкомасштабну і планомірну інформаційно-психологічну операцію. Монополізуючи символ Перемоги, паразитуючи на атрибутах та образах Другої світової війни, зловживаючи термінологією, візуальним наповненням та риторикою, кремлівські ідеологи формують у вигідному для себе світлі паралелі та конструкції, які стають живильним інформаційним підґрунтям для подальшої ескалації конфлікту. Домінування фейкових кейсів та версій у публічному дискурсі з приводу пам'яті про війну є ключовим елементом в реалізації інформаційної політики російських ідеологів. Сформований пропагандистами “русского мира” законсервований інформаційно-комунікаційний простір має деструктивний вплив на ідеї, світогляд, ціннісні орієнтири, та культурні компоненти свідомості тамтешніх мешканців. В результаті цього, серед українських громадян на підконтрольних та непідконтрольних територіях з'явилися певні відмінності в оцінці політичної ситуації та конфлікту на Сході України, ставленні до історичної минувшини та культури пам'яті. Інформаційно-психологічні акції кремлівських агітаторів-пропагандистів з кожним днем створюють дедалі складніші умови для деокупації і реінтеграції інформаційного простору окремих районів Донецької та Луганської областей.

**Метою статті** є оцінка пропагандистських кампаній в сфері політики пам'яті про Другу світову війну, які проводять ідеологи “русского мира” на тимчасово окупованій території України для протидії гібридно-месіанській агресії Кремля.

**Виклад основного матеріалу.** Після захоплення влади, образ Другої світової війни став для самопроголошених республік одним із головних концептів з консолідації і легітимізації окупаційного режиму, покликаних довести історичну тяглість приналежності Донбасу до “русского мира”. Пропагандисти та ідеологи з перших днів конфлікту, охрестивши українську владу, ЗСУ та населення західних областей України “київською хунтою”, “нацистами”, “фашистами”, “бандерівцями” та іншими подібними епітетами, почали форсувати порівняння дій нацистської Німеччини з воєнним конфліктом на Сході України. Відвертий хейтспітч активно увійшов до інформаційного поля через теле- та радіо ефіри, періодичні видання, та виступи ватажків “республік” на мітингах та масових зібраннях. Згадані штампи та інші міфи, які використовуються російськими пропагандистами на непідконтрольній Україні території, з року в рік підживлюються та домінують в інформаційних потоках, створюючи для реципієнтів вкрай негативний, емоційно забарвлений образ “кровожерливого ворога” у паралелі з подіями Другої світової війни.

Ідеологи “русского мира” на окупованій території України в Донецькій та Луганській областях активно використовують в своїх кампаніях термінологію та символіку періоду Другої світової війни, формуючи викривлений інформаційний простір за рахунок привласнення вирішальної ролі у розгромі нацизму винятково російському народові, та конструюванню ворожого, демонічного образу примарних “українацистів”.

Аналіз проведених масових заходів до 9-го травня з 2014 до 2019 рр. дає підстави вважати, що ватажки незаконних збройних формувань відпрацьовують заздалегідь затверджені сценарії. Використання значної кількості відомих методів та прийомів інформаційно-психологічних операцій та пропагандистських акцій вказує на те, що

посадовці самопроголошених “республік” керуються чіткими та вивіреними інструкціями з Російської Федерації.

Комплексна візуальна пропаганда, яку реалізують у так званих “ДНР” та “ЛНР”, має на меті сформувати інформаційний простір, який залишає у свідомості населення елементи невербальних кодів та кліше, вигідних для російського ідеологічного центру. Одним з інструментів візуалізації виступає плакат. Активна експлуатація плакатного формату агітаторами “русского мира” розпочалася задовго до початку вторгнення російських військ на схід України. Ще перед появою “зелених чоловічків” на українській землі у пропагандистській сфері регіону доволі наступально та агресивно використовувалися плакати періоду Другої світової війни з метою латентного розпалювання ворожнечі за сприяння “Інтеграційного комітету “Россия – Донбасс” – структури, діяльність якої, нібито, спрямована на посилення процесів гуманітарної, соціальної та культурної інтеграції Донбасу і Російської Федерації. Координатором комітету виступає і залишається у цій іпостасі депутат Державної Думи РФ Андрій Козенко [1]. Саме в межах роботи згаданого пропагандистського новоутворення 5 вересня 2017 р. у Донецькому краєзнавчому музеї відкрилась виставка “Плакати Великої Вітчизняної війни”, де експонувалися креолізовані тексти з фондів Державного меморіального музею Олександра Суворова (Санкт-Петербург) [2] у супроводі підтекстів, спрямованих на формування відповідного асоціативного ряду навіювання ворожого ставлення до українських військовослужбовців. Подібні акції винятково пропагандистського характеру проводилися на території самопроголошених “республік” систематично. Ця ж пересувна виставка неодноразово демонструвала свої експонати і в інших містах на тимчасово окупованій території України.

Організатори згаданих “вернісажів” особливо й не приховують своїх цілей та завдань. Так, в.о. начальника відділу охорони культурної спадщини так званого “міністерства культури ДНР” Н. Коваль на відкритті виставки зазначила: “Символічно, що виставка “Плакати Великої Вітчизняної війни” з фондів Державного меморіального музею О. Суворова відкрилася в Донецьку напередодні Дня визволення Донбасу від німецько-фашистських загарбників. Плакати того часу перегукуються з днем сьогоднішнім. Впевнена, що ці видатні твори підтримають дух воїнів ДНР і мирних жителів, вселяють в них упевненість у перемозі” [3]. Організатори розраховували на те, що виконуючи роль джерела інформації, залучені плакати і карикатура виконують функцію ретранслятора ідеологічних установок і запрограмують моделі поведінки та визначені ціннісні орієнтири для місцевого населення.

Так, серед представлених 51-ї копії плакатів із зібрань петербурзького музею, які латентно нав’язували асоціативний ряд з подіями на Сході України, були представлені плакат Кукриніксів “Нещадно розгромимо і знищимо ворога”, “Смерть німецько-фашистським загарбникам”, “Убий фашиста-нелюда”, “Воїн Червоної Армії – помстися ворогові за кров і сльози радянських людей!”, “Смерть дітовбивцям!”. Організаторами та ідеологічними натхненниками згаданого “бієнале” увага відвідувачів фокусувалася на плакатах із закликами до робітників та інженерів щодо збільшення випуску зброї: гвинтівок, автоматів, кулеметів, мінометів, знарядь, снарядів.

“Працювати в тилу, як на фронті”, “Кожна тонна хліба, вугілля, сталі – удар по ворогу” – подібні гасла-заклики активно інтегрувалися російськими ідеологами до інформаційного простору з 2014 р. в форматі біл-бордів, які розміщувалися на центральних вулицях окупованих міст. Подекуди, пропагандисти навіть не змінювали підтекстівки, а додавали лише триколори самопроголошених “республік”. Подібні акції активно використовуються ідеологами “русского мира” з метою апеляції до

сформованих архетипів сприйняття ще за часів СРСР, адже для більшості реципієнтів, плакатні образи “Батьківщини матері” та “воїна визволителя” мають виключно позитивні конотації, однак, у викривленому інформаційно-психологічному полі вони набувають властивостей, якими проросійські сили намагаються маніпулювати та “перефарбовувати” “чорне в біле”, а “біле в чорне”. Характерно, що широкоформатні зображення для біл-бордів, надходять для самопроголошених “республік” з Ростова-на-Дону. У такий спосіб російські пропагандисти використовують плакатну продукцію в якості інформаційної зброї, завдяки якій формується світогляд громадян і ведеться ідеологічна боротьба проти України.

Системний підхід до аналізу залучених ідеологами креолізованих текстів дає змогу розглянути мистецтво плаката і карикатури як технологію культурного продукування в контексті співвідношення традиційного та інноваційного в культурі. Агітаційно-пропагандистську систему впливу на свідомість і підсвідомість широких верств населення, та, головним чином, як інструмент формування інформаційного простору й апеляції до архетипів сприйняття в складному процесі латентної маніпуляції масовою свідомістю.

Ідеологи інформаційно-психологічного фронту самопроголошених новоутворень, активно використовують технологію візуального впливу в контексті психологічної війни. Завдяки штучно сконструйованим маніпулятивним технологіям, навіюванню штучних аналогій агресивно нав’язують поведінкові моделі та стереотипне, упереджене ставлення до “не наших”, чітко розмежовуючи та формуючи образи “своїх” і “чужих”. Усталені текстові стратегії, зокрема метафора, використовуються в пропагандистських кампаніях, аби справити візуальні або текстові/візуальні еквіваленти, що, в комбінації з малюнком і мовним елементом створюють привабливий або переконливий вплив на цільову аудиторію.

Очільники ідеологічних центрів самопроголошених “республік” крізь призму завдань, які ставлять їм московські куратори та місцеві “ватажки”, з одного боку свідомо звужують розуміння інформаційної сутності креолізованого тексту, з іншого – наповнюють його широким – замовним смисловим змістом.

Активне перенасичення інформаційного простору символами Другої світової, апелює у такий спосіб до традиції, пам’яттевої культури в якій День Перемоги займає визначне місце, а його репрезентатором, одноосібним монополістом на спадщину і “лаври” є РФ.

“Велика перемога” в окупованих містах презентується ідеологами-пропагандистами як ідеал мужності і героїзму, притаманний винятково “радянському народу” і його спадкоємцям. Пропагандисти на місцевому рівні усіма доступними методами нав’язують населенню Донбасу особливу самоідентифікацію, називаючи тамтешніх мешканців “людьми великого русского мира”, “радянським народом”, “народом російським”, “русским”. Ці елементи аудіо-візуального впливу на масову свідомість проектується на еволюції внутрішньо – і зовнішньополітичної лінії Кремля.

Окрім того, лідери незаконних збройних формувань, які активно використовують різноманітні теле- та радіопрограми за участі ветеранів, проводять генеральну тезу про необхідність об’єднання з Росією: “Жили як одна сім’я в Радянському Союзі. Так потрібно знову жити. Це єдиний шлях для нас” [4].

Експлуатуючи стереотипи масової свідомості, символіку й асоціації у прийнятній та зрозумілій для більшості адресатів образній формі кремлівські пропагандисти ретранслюють ідеологічні установки на різні категорії учасників і сучасників війни, формуючи не тільки уявлення про події, спосіб світосприйняття, а й моделі поведінки

мешканців незаконних новоутворень. Фіксуються масові випадки порівняння збройного конфлікту на Сході України з “Великою Вітчизняною”. Прикладом може слугувати захід “Діалог поколінь”, проведений 20 лютого 2020 р. “міністерством інформації ДНР”. У виступах нав’язливо повторювалися тези – пропагандистські кліше: “Війна в Донбасі – громадянська, і ворог у нас внутрішній, який виник через розкол суспільства. Жителі Донбасу продемонстрували всьому світу – ми не сепаратисти, ми боремося за мир, за Батьківщину, за свої родини і захищаємо свою Вітчизну” [5]. Головну ідею подібних акцій та заходів озвучив генерал-лейтенант В. Кононов, який займає посаду “начальника Управління з соціальної підтримки військовослужбовців у відставці і патріотичного виховання при главі ДНР”: “Захід такого широкого формату напередодні 75-річчя Великої Перемоги налаштує необхідним чином не лише молодь, яка захищає Донбас від укронацистів, а й допоможе цивільному населенню, яке повинне знати історію нашої перемоги, історію, яку не можна вбити, викоринити, адже наші люди повинні бути стійкими у своїх переконаннях” [6].

У візуальній пропаганді вирішальне значення мають психологічні процеси, емоції і почуття, які нею викликаються, активізуються та поглиблюються. Кремлівські пропагандисти вдало та ефективно використовують у своїх кампаніях маніпулятивні практики. Широкий спектр засобів такого навіювання пробуджує в пам’яті населення, яке опинилося під потужним ідеологічним пресингом, елементи, що викликають/стимулюють бажану для влади психологічно-емоційну реакцію на певні атрибути і символи. Все це загалом запускає у свідомості процеси асоціативних рядів та порівнянь, а відтак і стимулюючих установок для майбутньої потрібної дії.

Щороку напередодні Дня перемоги в ОРДЛО масово розповсюджуються плакати та з’являються біл-борди – червоного кольору з обов’язковим атрибутом – “георгіївською стрічкою”. Її чіпляють на автомобілі, надягають журналісти і телеведучі, роздають перехожим і пенсіонерам.

Чорно-помаранчева георгіївська стрічка стала одним із найголовніших атрибутів належності до “руського мира”, з 2005 р. вона була введена у вжиток в Російській Федерації та інших пострадянських країнах як основний символ перемоги Червоної армії над фашизмом.

У лютому 2014 року георгіївські стрічки отримали нові конотаційні смисли – їх активно використовували учасники руху “Антимайдан”, щоб підкреслити тим самим свою “антифашистську” і проросійську позицію [7]. Під час святкування Дня Перемоги у 2014 р. в самопроголошеній “ДНР” ідеологи-пропагандисти потурбувалися про те, аби забезпечити символікою всіх учасників святкових заходів. Окрім того, місцеве керівництво та ідеологічні служби ефективно використали урочистості 2014 р. у власних корисливих цілях. У своїх промовах політики нагадували, що наближається референдум про державний суверенітет Донецької області і закликали народ зробити єдино “правильний” політичний і моральний вибір, проводячи аналогії з подіями Другої світової війни, силою духу предків-переможців, “братерської єдності”.

За аналогічним сценарієм розвивалися події і у так званих “ЛНР”. Після референдуму, 12 травня, представники “ЛНР” оголосили суверенітет і висловили бажання вступити до складу Російської Федерації, а також об’єднатися з “Донецькою Народною Республікою” в “Новоросію” [8]. До речі, бюлетені, які використовувалися під час голосування, були розроблені одним виконавцем. На бюлетені в “ЛНР” для візуального обрамлення було використано георгіївську стрічку.

З метою легалізації нового символу Дня Перемоги, а також намагаючись затерти та знівелювати пам’ятні дати України в “ДНР”, зумисно, замість 6 грудня, коли ще з



1993 р. в Україні відзначається День Збройних сил України, російські політтехнологи у 2015 р. створили нову “пам’ятну дату” – “День георгіївської стрічки”. Перший заступник керівника виконкому так званого громадського руху “Донецька Республіка” А. Крамар заявив: “Сьогодні в Україні відзначають День збройних сил. Це робиться цілеспрямовано, тому в нашій молодій Республіці крім традиційних свят виникають нові – такі, як День георгіївської стрічки. І ці свята зможуть об’єднати всіх жителів ДНР” [9]. Ідеологи намагаються вкласти у свідомість населення хибний код візуального об’єкту – стрічки, як символу спадкоємності поколінь, прихильності до миру і головного візуального символу антифашистського руху.

Абсолютно скрізь на тимчасово окупованих Росією територіях головним “об’єктом виховання” є діти та молодь. Затяжна війна дає можливість ідеологам “руського мира” підкріплювати політичну риторику “ЛДНР-івських пропагандистів”, які наполегливо і послідовно репрезентують тамтешньому населенню поточний конфлікт як визвольну боротьбу обложеної “київськими фашистами народної республіки”.

Разом з тим, спираючись на місцеву меморіальну традицію, регіональні політики оголошують сьогоднішній конфлікт “прямим продовженням визвольної Великої Вітчизняної війни”. Це здійснюється за допомогою трансляції проекції історичної пам’яті про минулу війну на сучасний конфлікт, формування єдиного дискурсивного поля з високим мобілізуючим потенціалом. Як зазначають дослідники Й. Хелльбек та Д. Титаренко, “драматизм історичної спадкоємності багаторазово посилюється в тих випадках, коли поточні військові дії проходять на історично пам’ятних, що володіють “сакральною” знаковістю, місцях боїв Червоної армії і німецького Вермахту. Сліди руйнувань на постраждалих в нинішній війні пам’ятниках немов реактивують їх символічну силу” [10].

Присвячена 70-й річниці Перемоги агітаційно-пропагандистська кампанія, за задумом ідеологів, мала сформувати відчуття спільної історичної долі та згуртувати учасників меморіальних урочистостей в однорідну масу прихильників патріотичної ідеології. Як відзначають дослідники, історична пам’ять про минулі битви стала частиною самоідентифікації жителів регіону, штучно ушляхетнивши і легітимізувавши роль бойовиків в конфронтації з “Київською хунтою”. Взаємопроникнення минулого і сьогодення підвищило релевантність населення у сприйнятті пропагандистських гасел місцевих та російських ідеологів [10].

Паради та святкові гуляння, приурочені до Дня Перемоги, стали в “республіках” одними з наймасовіших з часів СРСР і завжди закінчуються святковим феєрверком [11]. Ідеологи та організатори усіяко намагаються створити атмосферу народного свята з використанням усього можливого арсеналу. І треба визнати, що це їм вдається. Тим часом риторика та меморалізаційні заходи, присвячені “Дню Перемоги”, на жаль, стають живильним підґрунтям для подальшої ескалації конфлікту.

Завдяки відповідним зусиллям місцевих ідеологів та за дієвої підтримки “колег” з РФ, вже від 2016 р. військові паради до Дня Перемоги стали дієвою та масштабною пропагандистською атракцією. у 2016 р. приміром, у Луганську 9 травня з Театральної площі пройшли близько 1 тис. осіб і близько 70 одиниць військової техніки. Крім військових у параді брали участь співробітники правоохоронних органів і кадети. Завершували ходу учасники акції “Безсмертний полк” з фотографіями своїх родичів, загиблих під час Другої світової війни. У порівнянні з першим парадом до ювілею перемоги, проведеним у 2015 р., наступного року республіка відзначала свято скромніше. Тоді центральною площею міста урочистими лавами пройшли близько 800 військових, а колона бронетехніки налічувала 30 машин.

У Донецьку 2016 р. в святковій ході взяло участь 45 одиниць бойової російської техніки, зокрема бронетранспортери БТР-80, танки Т-72, системи залпового вогню “Град” і самохідні гаубиці “Гвоздика”. Крім сучасної техніки в заходах були представлені бойові машини часів Другої світової війни. У складі парадної колони пройшла установка “Катюша”. Завершували хід, так само як і в Луганську, учасники акції “Безсмертний полк”.

З 2017 р. День Перемоги став дедалі помітніше поступатися в масовості святкуванню так званого “Дня республіки”. Урочисті заходи, і парад, і акція “Безсмертний полк”, і військова музика, і 50 грамів “фронтових” продовжують наливати біля пам’ятників, однак 9 травня перетворилося на своєрідну “премедикацію” для більш заідеологізованої акції святкування. На вулицях ОРДЛО в середньому на один вітальний біл-борд до Дня Перемоги стало припадати три “З днем республіки”. Варто зазначити, що пропагандистську акцію “Безсмертний полк” в “ДНР” “очолили” фотографії так званих “героїв республіки” – О. Немогає (прізвище “Алекс”), М. Толстих (псевдо “Гіві”) і А. Павлова (прізвище “Моторола”).

Вже традиційно акції вшанування 9 травня в “ЛДНР” закінчуються пісню “Хотят ли русские войны”, а майже всі масові заходи, які проводяться з 2015 р., перегукуються з “Планами культурних програм, присвячених Перемозі у Великій Вітчизняній війні 1941 – 1945 років в Москві, адміністративних центрах суб’єктів Російської Федерації, містах-героях, містах військової слави” [13].

У 2018 р. самопроголошений “міністр оборони ДНР” В. Кононов на урочистостях до “Дня Перемоги” заявив, що вони збираються “рівнятися на Росію”. Це повністю відповідало візуальній картинці під час проведення всіх меморіальних акцій. Ватажок ЛНР Л. Пасічник виголосив традиційну нетривалу промову про “могутність російського народу”. Після цього вулицями пройшла військова техніка. На початку колони йшли танки часів СРСР, а за нею – сучасна російська техніка: БМП, БТР-80, 122-мм самохідні артилерійські установки “Гвоздика”, 152-мм гаубиці “Мста-Б”, 122-мм гаубиці Д-30, реактивні системи залпового вогню “Град”, зенітно-ракетні комплекси “Стріла-10”. Після цього бюджетники добровільно-примусово пройшлися в рядах “Безсмертного полку”. Варто відзначити, що колона була значно коротшою, ніж у 2017-му, коли І. Плотницький змушував людей ходити по колу, щоб створити видимість масовості. Про те, що основним ідеологічним орієнтиром та донором є РФ, свідчать і слова представника так званої “народної міліції ЛНР” – А. Марочка, який заявив: “Упевнений, наші військовослужбовці йшли не гірше, ніж на самому головному параді в Москві” [13].

У 2019 р. на 74-ту річницю Перемоги в “ЛНР” були заплановані переважно ті ж самі традиційні акції, що й у попередні роки. Головним нововведенням став новий захід, запущений за ініціативи так званої “народної міліції ЛНР” – танковий вальс. Цінність “танцю” полягає в технічних елементах, які дуже складно виконати на танку в ритм музики [14]. На 2020 р. припадає ювілей – 75 річниця перемоги, незважаючи на пандемію і карантин через COVID-19, в “ЛНР” не скасували проведення парадів до 9 травня, однак поступово закривають міста на самоізоляцію. У “ДНР” 17 квітня все ж заявили про перенесення парадів до 9 травня на невизначений термін.

Форма святкування з використанням відповідних символів є одним із засобів впливу, що спрямований на створення й цементування певних ціннісних установок у свідомості мешканців самопроголошених “республік”. Механізм цього впливу – в ретрансляції потрібної цільової інформації, формування на її основі уявлень про

оточуючу дійсність, інтересів та потреб аксіологічних та світоглядних орієнтирів громадян, і врешті-решт, стимулювання їх до певних дій.

Процес сприйняття та розуміння візуальних пропагандистських образів і текстів у рамках “свої – для своїх” та “свої – для чужих”, де “своїми” оголошені виключно РФ – має суттєві відмінності. Головним чинником та необхідною умовою не тільки розшифрування коду, а й очікуваної реакції на нього, виступає особиста політична позиція адресата, його ставлення до явищ, подій та персоналій. У першому випадку реципієнт, як правило, відчуває довіру до “своїх” і налаштовується на схвалення та підтримку ідеї того чи іншого заходу (хоча мають випадки опозиції). У другому, – навпаки, домінуючими настроями виступають пересторога, недовіра, упередження до того, що надходить зі стану “чужих” (і в цьому разі чимало людей виявляють більшу довіру до “чужих”, якщо не довіряють “своїм”).

### **Висновки.**

Аналіз заходів, приурочених до святкування Дня перемоги, дає підстави дійти певних висновків.

Тотальна обробка масової свідомості у поєднанні з мілітаризацією самопроголошених новоутворень поступово перетворює тамтешніх мешканців на слухняний, покірний натовп, який сліпо вірить кремлівським ЗМІ та акціям, які проводять ідеологи-пропагандисти.

Очевидно, що маніпулятивні та пропагандистські підходи в експлуатації пам’яті про Другу світову війну формують на території так званих “ЛДНР” специфічний інформаційний простір, який забезпечує незаконним збройним формуванням необхідний рівень підтримки серед місцевого населення, а також виховує ціле покоління молоді із деформованим уявленням як про події Другої світової війни, так і вороже ставлення до України та усієї західної цивілізації. Пропагандисти використовують і конструюють пам’ять про жертви масового насильства Другої світової війни для виправдання сучасного і майбутнього кровопролиття, а агітаційно-пропагандистські акції, приурочені до святкування Дня Перемоги, формують зручне підґрунтя для подальшої ескалації конфлікту.

Як вважаємо, певні аспекти, які визначені у статті можуть бути корисними для врахування під час деокупації і реінтеграції інформаційного простору.

### **Використана література**

1. Интеграционный комитет “Россия – Донбасс”. URL: <http://russia-donbass.ru/o-nas>
2. В Донецке открылась выставка плакатов времен Великой Отечественной войны. – (Правительство Донецкой Народной Республики). URL: <https://pravdnr.ru/v-donecke-otkrylas-vystavka-plakatov-vremen-velikoj-otechestvennoj-vojny>
3. В Донецке открылась выставка “Плакаты Великой Отечественной войны” из фондов Государственного мемориального музея Александра Суворова (г. Санкт-Петербург). – (Министерство культуры ДНР). URL: <http://mincult.govdnr.ru/news/v-donecke-otkrylas-vystavka-plakaty-velikoy-otechestvennoy-voyny-iz-fondov-gosudarstvennogo>
4. День победы: мифы российской пропаганды на Донбассе URL: <https://www.RadioSvoboda.org/a/29214944.html>.
5. Жители Донбасса не сепаратисты! Белые журавли. URL: <http://podvig-dnr.ru/zhiteli-donbassa-ne-separatisty-my-zashhishhaem-rodinu-veteran-vov-vladimir-sheludko-video>
6. 75 лет Великой Победы. *Комсомольская правда*. URL: <https://www.donetsk.kp.ru/daily/75-let-pobedy>
7. Das Georgsbändchen: Was es verbindet, was es trennt. Erinnerungskulturen URL: <https://erinnerung.hypotheses.org/28>

8. ДНР и ЛНР выразили желание войти в состав России. *Газета.Ru*. URL: [https://www.gazeta.ru/politics/news/2015/06/10/n\\_7275741.shtml](https://www.gazeta.ru/politics/news/2015/06/10/n_7275741.shtml)

9. Митинг в честь Дня георгиевской ленты собрал в Донецке 5 тыс. горожан. – (Донецкое агентство новостей). URL: <https://dan-news.info/obschestvo/miting-v-chest-dnya-georgievskoj-lenty-sobral-v-donecke-5-tys-gorozhan.html>

10. “Мы победим, как победили 70 лет назад наши деды и прадеды”. Украина: празднование Дня Победы в тени новой войны. *Новое литературное обозрение*. URL: [https://www.nlobooks.ru/magazines/neprikosnovennyu\\_zapas/108\\_nz\\_4\\_2016/article/12112](https://www.nlobooks.ru/magazines/neprikosnovennyu_zapas/108_nz_4_2016/article/12112)

11. Глава ЛНР: На Параде Победы мы показали единство со всем русским миром. URL: <https://eadaaily.com/ru/news/2015/05/10/glava-lnr-na-parade-pobedy-my-pokazali-edinstvo-so-vsem-russkim-mirom>

12. План культурных программ, приуроченных к 70-летию Победы в Великой Отечественной войне 1941 – 1945 годов, в Москве, административных центрах субъектов Российской Федерации, городах-героях, городах воинской славы. – (Министерство культуры Российской Федерации). URL: <https://www.mkrf.ru/documents/plan-kulturnykh-programm-priurochennykh-k-70-letiyu-pobedy-v-velikoy-otechestvennoy-voyne-1941-1945>

13. В Луганске прошел Парад Победы. URL: <https://ria.ru/20180509/1520219263.html>

14. Танковый вальс, бал Победы и концерт артистов из РФ пройдут в Луганске 9 Мая. – (Государственная телевизионная и радиовещательная компания Луганской Народной Республики). URL: <https://gtrklmr.com/2019/04/27/tankovyj-vals-bal-pobedy-i-koncert-artistov-iz-rf-projdut-v-luganske-9-maya-mksm>

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

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

УДК 341.3+344.1(477)

ЯЩЕНКО В.А., доктор юридичних наук, професор, головний науковий співробітник
НДІ інформатики і права НАПрН України.
ORCID: <https://orcid.org/0000-0002-2257-318X>.

ВІЙСЬКОВЕ ПРАВО: ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ

Анотація. У статті йде мова про сутнісно-змістовні аспекти військового права як специфічної сфери регулювання військових відносин. Головна увага приділяється висвітленню та узагальненню теоретичних положень здобутків науковців та практиків у цій сфері, а також здійснено критичний аналіз наявних методологічних підходів і висновків, що стосуються виявлення та обґрунтування закономірностей військового права. Висунута та обґрунтовується теза про пріоритетність військово-оборонної складової військового права як його головного сутнісно-змістовного чинника, який, власне, і повинен визначати правову парадигму військового феномену.

Ключові слова: військове право, сутність військового права, військові відносини, оборона країни, військовий обов'язок, галузь права.

Summary. The article deals with the substantive aspects of military law as a specific area of regulation of military relations. The main attention is paid to the coverage and generalization of theoretical positions of achievements of scientists and practitioners in this field, as well as a critical analysis of existing methodological approaches and conclusions concerning the identification and justification of the laws of military law. The thesis about the priority of the military and defense component of military law as its main substantive factor, which, in fact, should determine the legal paradigm of the military phenomenon, is put forward and substantiated.

Keywords: military law, the essence of military law, military relations, national defense, military duties, the branch of law.

Аннотация. В статье рассматриваются предметные аспекты военного права как особой области регулирования военных отношений. Основное внимание уделено освещению и обобщению теоретических позиций достижений ученых и практиков в этой области, а также критическому анализу существующих методологических подходов и выводов, касающихся выявления и обоснования законов военного права. Выдвигается и обосновывается тезис о приоритетности военно-оборонительного компонента военного права как его основного содержательного фактора, который фактически должен определять юридическую парадигму военного явления.

Ключевые слова: военное право, сущность военного права, военные отношения, оборона страны, военные обязанности, отрасль права.

Постановка проблеми. Останнім часом до висвітлення проблем військового права звертаються чимало дослідників, які у своїх працях розглядають, як правило, фактологічні аспекти, аналізуючи його повсякденну практику традиційно в частині організації діяльності збройних сил. При всій позитивній оцінці їх здобутків все ж відзначимо, що в цій практиці превалує емпіричний рівень досліджень, який веде до накопичення знань, але без їх теоретичного узагальнення вони не синтезують нового знання.

Між тим, нині ця потреба є нагальною, оскільки актуалізує необхідність розробки теоретико-методологічної парадигми даної сфери. Саме такий підхід, на нашу думку, дасть можливість констатувати досягнуте, і сприятиме подальшому розвитку військового права.

Ці питання, а також спроба відповіді на актуальні проблеми військового права – предмет розгляду даної статті.

Результати аналізу наукових публікацій. У наявних публікаціях з військового права мають місце спроби як доктринального його розгляду, так і співвідношення з іншими галузями права. Тривалий час ця проблема залишається предметом дослідження П.П. Богущького, О.О. Гущина, І.Ф. Коржа, А.І. Коропатніка, В.Г. Пилипчука, С.М. Скуріхіна, І.М. Шопіної, В.В. Шульгіна, та багатьох інших авторів, праці яких сприяли значною мірою відновленню інтересу до цієї галузі права, зробили вагомий внесок у понятійно-категоріальний апарат військового права.

Слід також позитивно відзначити видання підручника “Військове право” авторського колективу Військового інституту Київського національного університету імені Тараса Шевченка, яким зроблена спроба класифікувати військове право у межах категорій загального, особливого та спеціального [1].

Військово-службові правовідносини, їх характерні риси розкриваються у публікаціях І.Ф. Коржа. Він підтримує думку значної частини фахівців у тому, що “усі ці відносини мають управлінський характер і в значною мірою охоплені адміністративно-правовим регулюванням” [2, с. 98].

І.І. Гибалюк, С.Г. Головка, В.С. Шаріпова висувають ідею наявності інститутів військового права, зокрема, таких як: інститут військового обов’язку, інститут мобілізації, інститут військової служби за контрактом, інститут альтернативної служби, інститут речового забезпечення, інститут атестації військовослужбовця, інститут виконання наказу та ін. [3, с. 54-55].

І.М. Шопіна, О.О. Гущин розглядають питання сучасного стану розвитку військового права як науки і навчальної дисципліни і обґрунтовують потребу критичного переосмислення системи наукових поглядів на існування воєнного права як галузі законодавства та науки [4]. Досить пізнавальними є думки В.В. Шульгіна стосовно реалізації військового права та історичні екскурси в генезу його розуміння [5].

Аналіз публікацій дає підстави вважати, що існує нагальна потреба здійснення узагальнено-теоретичного аналізу феномену військового права і висвітлення його методологічних засад, що донині не знайшло свого належного вирішення у дослідженнях вітчизняних авторів.

Метою статті є висвітлення в контексті діалектичного методологічного підходу визначально-регулятивних складових військового права.

Виклад основного матеріалу. Звернення до теоретико-методологічного аналізу військово-правової парадигми зумовлене декількома обставинами. По-перше, до цього змушує сам феномен військового права, місце та роль якого в регулюванні сучасних збройних конфліктів суттєво зростає. Між тим, ці обставини ще не спонукали фахівців до предметного теоретичного розгляду цих питань, хоча, як свідчать останні події, пов’язані з агресією Росії проти України без залучення військово-правової складової, вирішення цього конфлікту неможливе.

Друга обставина пов’язана з необхідністю відновлення та подальшої розробки теорії військового права України, яка свого часу була безпідставно призупиненою. Мова йде про військове право як науку.

Як відомо, усі без винятку дослідники розглядають військове право як своєрідну тріаду у єдності трьох складових: по-перше, як галузь права, що регулює сферу військових відносин; по-друге, як науку (сфера правознавства) і по-третє, як навчальну дисципліну, що викладає військове законодавство.

Проте всі ці складові містять масу невирішених проблем, зокрема, питання військового права як галузі права залишається дискусійним, у свою чергу військове законодавство як навчальний предмет не може, вважаємо, повноцінно замінити всієї військово-правової реальності, яка є більш загальною по відношенню до законодавства. Формою суспільної свідомості, як відомо, є право, а не законодавство, яке врешті-решт є закономірним результатом реалізації права.

Щодо військового права як науки. то спочатку воно входило до переліку наукових спеціальностей. Однак, згідно з наказом Вищої атестаційної комісії України у 2000 році ця спеціальність була ліквідована. Це, призвело до зниження теоретичного і практичного рівня досліджень у військово-правовій сфері і значно загальмувало розвиток військового права як науки. У грудні 2018 року Міністерство освіти і науки України відновило своїм наказом цю спеціальність, ввівши її до складу юридичних наук.

Слід зауважити, що існування трьох складових військового права в цій тріаді не рівноцінне. Наукова складова не є самодостатньою. Вона значною мірою – чинник подальшого розвитку військового права і як галузі права і як навчальної дисципліни.

Саме гальмування військового права як наукової теорії, вважаємо, призводить до того, що в ньому дедалі більше накопичуються теоретичні прогалини, зокрема, не виявляється своєрідність та унікальність військового права, заповнення яких віддається на відкуп іншим галузям права – адміністративного, цивільного, господарського тощо, що негативно відбивається на розвитку військового права і правознавства як навчальної дисципліни.

У зв'язку з цим необхідно відзначити важливість застосування та подальшої розробки науково зваженої методології військового права, зокрема, з'ясування співвідношення військового права з зазначеними феноменами як в сутнісно-змістовному, так і в практичному аспектах.

Однією з перших теоретико-методологічних прогалин, які потребують нагального вирішення, є визначення поняття військового права, яке в повсякденному вжитку трактується як “право військової сфери”. На наш погляд, це не стільки наукове, скільки буденне розуміння військового права. Такий підхід має місце в окремих публікаціях: “Право військової сфери (військове право) – сукупність правових норм, якими регулюються суспільні відносини у сфері функціонування Збройних Сил та інших військових формувань України” [6, с. 81].

Крім буденних уявлень про військове право в літературі зустрічаються дефініції, які оцінюють його як комплексну галузь права. Так, у підручнику “Військове право” за редакцією І.М. Коропатніка, І.М. Шопіної дається наступне його визначення: “Військове право України є комплексною галуззю національного права, здійснює регулювання військово-публічних відносин, суб'єктами яких є не лише військовослужбовці, але спеціально визначені законом органи державної влади та управління, військові частини та установи, органи військового управління” [1, с. 18].

Цікавою у дослідників є кваліфікація військового права як комплексного і, так би мовити, дещо гібридного явища. Для військового права, зазначають вони, “характерним є наявність “прикордонних зон”, тобто, регулювання одних і тих же питань різними галузями права” [7, с. 10]. Ці визначення військового права не можна кваліфікувати як

хибні, вони так чи інакше відзначають окремі складові цього феномену. Ми ж констатуємо лише їх неповноту.

Такі визначення в принципі правомірні, але вони настільки загальні (правовідносини), що не розкривають особливостей саме військового права. Між тим, визначення поняття навіть з точки зору формальної логіки вимагає проведення двох логічних операцій: з'ясування родової належності явища, яке визначається та аналіз його видових, специфічних відмінностей. Таким чином, за своєю родовою належністю військове право відноситься до сфери регулятивних правових чинників і, безперечно, мають рацію ті автори, які підкреслюють саме цю ознаку, вказуючи на його суто правову природу.

Друга логічна операція – розкриття видових ознак військового права, перерахування його сутнісних характеристик, а саме те, що притаманне лише військовому праву і ніякому іншому. В такому разі військове право не може кваліфікуватись як комплексна галузь, бо його особливості, унікальність не будуть виявлені. Як вважає Г.В. Новицький “...потребує переосмислення ідея існування комплексних галузей права, оскільки сама природа галузі права ...виключає можливість існування комплексних галузей права на відміну від комплексних галузей законодавства. Одна правова норма не може регулювати різні за своєю правовою природою відносини, а твердження про наявність у галузі права норм інших галузей права лише заперечує її самостійність і ставить під сумнів можливість вважати таку сукупність правових норм галуззю права” [8, с. 263].

Вважаємо, що відзначенням саме сутнісних особливостей керується один із провідних дослідників цього феномену П.П. Богуцький, який зазначає, що “військове право є системою загальнообов’язкових формально визначених правил поведінки у військовій сфері, які встановлені та охороняються державою, регулюють суспільні відносини, що пов’язані з діяльністю воєнної організації суспільства і мають на меті забезпечення захисту держави, її суверенітету і територіальної цілісності” [9, с. 16].

Зазначимо, що у цьому визначенні, крім сутнісних характеристик, автор значною мірою вказує на його змістовно-функціональні атрибути, серед яких не лише регулятивність як визначальна родова належність військового права, а й вказівка на соціальні відносини, як детермінанту правобуття та правосвідомості.

На нашу думку, ці відносини не просто соціальні, вони конкретизуються у своїх головних характеристиках, до яких належать в першу чергу відносини воєнні. На цій характеристиці зупинимось більш детально. На жаль, більшість дослідників цю особливість відзначають дещо спрощено. “Військове право – пишуть вони, характеризується більшою у порівнянні з іншими галузями права деталізацією регулювання суспільних відносин, пов’язаних з функціонуванням військової організації держави” [7, с. 11].

Вірно, але зазначимо, що справа не лише в деталізації і, крім того, не зводиться лише до організаційної сторони. Вся справа у військових відносинах, зміст яких значно збагатився під впливом суворих реалій сьогодення, що не могло не відбитися на головній регулятивній функції військового права – військово-бойовій, оборонній.

У той же час цей критеріально-змістовний аспект військового права ще не знаходить, на нашу думку, належного обґрунтування. Тобто, військове право висвітлюється через призму його структури, джерел, соціальної складової тощо, а визначальні сутнісно необхідні аспекти – регламентація воєнних дій з забезпечення оборони країни, її територіальної цілісності та суверенітету майже не розкриваються. А між тим, саме цей аспект є специфічно унікальним, що і формує власне сутність військового права.

Так, у посібнику П.П. Богуцького, С.М. Скуріхіна “Основи військового права” досить повно висвітлені питання джерел, структури військового права, особливості військово-правових відносин та ін., а військово-операційна складова практично не розкривається [10]. Водночас П.П. Богуцький, об’єктивно вважаючи, що “визначення військового права ґрунтується на окресленні його ознак” зробив спробу виокремити ці основні ознаки, до яких, на його думку, належать: “нормативність, формальна визначеність, обов’язковість, регулятивність, процедурність, зв’язок з державою, системність” [11, с. 154-155].

Якщо взяти за основу загально правовий критерій, то очевидно, з таким підходом до визначення ознак військового права можна погодитися. Разом з тим, їх слід доповнити, вважаємо, ще й атрибутивними саме для військового права ознаками. Так, виходячи з сутнісної визначеності військових відносин їх атрибутивною характеристикою є воєнна складова, без якої військове право взагалі існувати не може. Тому однією з ключових ознак саме військового права є його воєнний характер.

По-друге, військові відносини володіють ознакою субординаційності, що зумовлює імперативний характер військового права, що теж є його невід’ємною ознакою. По-третє, на нашу думку, у чисто рафінованому вигляді по відношенню до цивільних зв’язків військові відносини не існують, вони навпаки, опосередковані ними. Тому поєднання цивільно-військових відносин теж є ознакою військового права. Вважаємо, що поєднання цих ознак і дає можливість визначити особливість військового права.

Ряд авторів публікацій з військового права (Т.Г. Каткова) [6, с. 81] пропонують розробку Військового кодексу, до якого рекомендують включити питання військової організації держави, комплектування Збройних Сил України, статусу військовослужбовців, їх відповідальності і т.п., а все ж вирішальний аспект – військово-операційний, правове регулювання ведення бойових дій не враховується.

На відміну від цього автори підручника з військового права Військового Інституту Київського національного університету імені Тараса Шевченка включили до його змісту питання “операційного права”, правової регламентації проведення військових операцій та ін., що є досить інноваційним у розумінні змісту військового права [1, с. 548].

Однак ці питання розглядаються не у загальній, чи особливій частинах, а відокремлено у спеціальній частині, тобто як одиничний прояв, а не в їх діалектичному зв’язку з загальною і особливою частинами. Таким чином, статус вирішальної складової військового права – ведення воєнних дій, військово-операційної складової, не отримує своєї фактичної належності.

Очевидно, саме через це автори статті з питань стану та розвитку військового права І.М. Шопіна та О.О. Гуцин зазначають, що в освітньо-професійній програмі Військового інституту Київського національного університету імені Тараса Шевченка “...перелік дисциплін спеціалізованої професійної підготовки складається з курсів, які дають розрізнені знання щодо особливостей окремих сфер правового регулювання діяльності Збройних Сил України (“Вступ до спеціальності”, “Військова адміністрація”, “Правова робота в Збройних Силах України”, “Право збройних конфліктів”, “Особливості військових злочинів”, “Військове документування і діловодство”) і не характеризується системним підходом” [4, с. 147].

Звідси основні змістовно-функціональні аспекти військового права, це, на наш погляд, в першу чергу визначення і регламентація практичного впровадження військової стратегії і тактики, мобілізаційної складової держави, розбудови Збройних Сил України, правове регулювання здійснення військових операцій, особливостей соціального захисту військовослужбовців тощо.

На нашу думку, одну з ключових закономірностей військового права, що розкриває ведення воєнних дій, воєнних операцій, доцільно розкривати через зміст Бойових статутів, адже "...бойові статuti визначають основи організації і ведення бою і принципи бойового застосування в ньому частин і з'єднань різних видів збройних сил. У бойових статутах видів збройних сил викладаються основи бойової діяльності їх з'єднань, частин і підрозділів в загальновійськовому бою і при веденні самостійних бойових дій" [12]. Наприклад, у загальновійськовому Бойовому статуті регламентуються питання пересування військових підрозділів, ведення наступального, оборонного, зустрічного бою, дій у міжнародних операціях з підтримання миру і безпеки, участі у стабілізаційних, специфічних діях військ та операції тощо, які, безумовно, без правової регламентації сьогодні неможливі [12, с. 5-12].

Вважаємо, що виокремлені воєнно-бойові аспекти і складають у своїй діалектичній єдності зміст військового права, що і виокремлює його з інших сфер правового регулювання суспільного життя і, разом з тим, детермінує їх на дотримання визначеної вище основної сутнісної характеристики військового права – військово-операційній, тобто, ведення воєнних (військових) дій.

Зрозуміло, що всій цій військово-професійній багатоманітності необхідно надати відповідну правову характеристику, так би мовити, військову стратегію і тактику вплести в правову тканину. Такий підхід, вважаємо, значно збагатить зміст військового права і сприятиме якісному оновленню його освітньо-виховної складової. Як зазначав ще більше 100 років тому А. Ертель, слід проявити "мистецтво застосовувати постанови воєнного права до конкретних випадків" [5, с. 120].

Розглядаючи сутнісно-змістовну складову військових відносин неможливо обійти їх атрибутивну властивість, притаманну лише їх правовій природі, а саме, те, що формою реалізації всіх зв'язків та опосередкувань є статuti, розпорядження, настанови, накази. Наказовість – невід'ємна риса існування військового права. Норми цих документів у військовому праві набувають статусу законів, іншими словами, суттєво закономірного явища, навіть у тому випадку, коли вони не лише писемні, а й усні.

Звичайно, ці наказові норми, як абсолютно визначені, носять імперативний характер бо є різновидом веління. В такому разі "одна із сторін має право вимагати від другої сторони такої поведінки, яка визначена адміністративно-правовою нормою і охороняється державою". Але в той же час як одна, так і друга сторона взаємно зобов'язані між собою, а також спільно виконують один і той же обов'язок – захист безпеки Батьківщини. Тобто, особа приймає на себе обов'язок "вчинити або утриматись від вчинення певних дій" [13, с. 298]. Цей морально-правовий аспект надає військовому праву особливий зобов'язальний зміст, що відрізняє його від інших сфер правового регулювання. Вважаємо, що ця, власне, екзистенційна закономірність військового права надає йому своєрідної унікальності, і разом з тим, життєстверджуючої буттєвості. На нашу думку, цей момент виводить військове право на рівень національного законодавства.

Ми тому так детально зупинились на з'ясуванні атрибутивної складової військового права, зокрема, регламентації ведення бойових дій, що всі відзначені закономірності притаманні як його предметності, так і характерні для його найбільш теоретико-узагальненої парадигми – методології.

Сьогодні проблема методологічного чинника військового права майже не розглядається. Між тим, ця методологія інтегральна за структурою та змістом і є своєрідним синтезом філософсько-правової, збройно-оборонної, військово-юридичної складових, яким вона керується, визначаючи військове право і забезпечуючи його розвиток. При цьому найбільш загальна філософсько-правова складова концентрує

увагу на діалектиці відношення військово-правової свідомості до військового правобуття, тобто до військових відносин. Зокрема, одним із уроків агресії Росії проти України (гібридної війни) є висновок про те, що військова правосвідомість, зокрема керівників держави, була фактично не готовою до катаклізму у сфері військового буття. Цей філософсько-правовий казус відіграв, як відомо, негативну роль у забезпеченні оборони країни.

Вважаємо, що своєрідну унікальну природу у військовому праві мають і спеціальні методи військово-наукового і військово-юридичного відображення дійсності. В першу чергу зазначимо, що військове право за своєю природою поєднує ці дві його складові, легітимізуючи застосування збройної сили у чітко визначених випадках, наприклад, оборони від агресора, відновлення територіальної цілісності держави та її суверенітету. Отже, при всій згубності наслідків збройного втручання війна об'єктивно не може не вестися в певних межах.

З урахуванням зазначеного підкреслимо, що головним все ж виступає метод упередження, запобігання збройного конфлікту. Військове право як підпорядковане загальним правовим закономірностям тяжіє не до конфлікту, тобто, до невирішуваних суперечностей, а виступає одним із засобів їх вирішення.

Вважаємо, що для військового права чи не найбільш характерна діалектика збройного та мирного насилля, де правове обмеження цього насилля відіграє роль методологічного принципу. На цьому, власне і будується вся система міжнародного гуманітарного права, у тому числі й національного військового права.

Висновки.

Військове право як теорія і як метод є особливим феноменом у системі права України, покликаним не лише науково зважено пояснити військове правобуття, військові правовідносини, а й, що не менш важливо, розкрити регулятивний, перетворюючий механізм дії військово-оборонної сфери держави. Тобто, військове право, на нашу думку, щоб бути інституційованим, має стати правом воєнним, хоча б у його суттєвій частині.

До аргументів на користь такої точки зору слід віднести і ті обставини, які є визначальними, необхідними. А саме, суто воєнні атрибути, характер сучасної війни (збройного конфлікту) і можливих майбутніх конфліктів і визначають власне, зміст та напрямки реформування Збройних Сил України. Очевидно, і саме військове право існує як рефлексія на ці процеси, а все інше є похідним від цього суттєвого, визначального. Із вищезазначеного можна зробити висновок про своєрідну унікальність військового права як способу регулювання військових відносин.

Використана література

1. Військове право: підручник / за ред. І.М. Коропатніка, І.М. Шопіної. Київ: Алерта, 2019. 648 с.
2. Корж І.Ф. Військове право та його місце в системі національного права: матеріали Міжнародної науково-практичної конференції *Система військової юстиції у забезпеченні національної безпеки України*, м. Київ, 2019 р. / упоряд: Пилипчук В.Г., Коваль В.П., Богущкий П.П., Беланюк М.В., Дорогих С.О., Доронін І.М., Радзієвська О.Г. Київ: Видавничий дім "АртЕк". 2019. С. 97-101.
3. Гибалюк І.І., Головка С.Г., Шаріпова В.С. Перспективи розвитку і сучасний стан військового права: матеріали XXVIII Міжнародної науково-практичної Інтернет-конференції *Пріоритетні напрями розвитку науки*, м. Вінниця, 18 берез. 2019 р. Вінниця, 2019. Ч. 1. С. 53-57.

4. Шопіна І.М., Гущин О.О. Актуальні проблеми сучасного стану розвитку воєнного (військового) права як науки і навчальної дисципліни. *Форум права*. 2017. № 2. С. 144-148. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2017_2_24

5. Шульгін В.В. Військова юстиція в Україні: генезис реалізації військово-правової концепції: матеріали Міжнародної науково-практичної конференції *Система військової юстиції у забезпеченні національної безпеки України*, м. Київ, 2019 р. / упоряд: Пилипчук В.Г., Коваль В.П., Богуцький П.П., Беланюк М.В., Дорогих С.О., Доронін І.М., Радзівська О.Г. Київ: Видавничий дім “АртЕк”. 2019. С. 117-128.

6. Каткова Т.Г. Військове право: сучасний стан і перспективи розвитку: матеріали науково-практичної конференції *Актуальні проблеми захисту прав та представництва законних інтересів військовослужбовців та військовозобов’язаних у кримінальному та адміністративному законодавстві України: сучасний стан та перспективи*, м. Харків, 11 груд. 2015 р. Харків: Харківський економіко-правовий університет, 2015.

7. Стрекозов В.Г., Кудашкин А.В. та ін. Военное право: учебник. Сер. “Право в Вооруженных Силах – консультант”. Москва: “За права военнослужащих”, 2004. Вып. 45. 640 с. URL: <https://may.alleng.org/d/jur/jur721.htm>

8. Новицький Г.В. Теоретико-правові основи забезпечення національної безпеки України: монографія. Київ: Інтертехнологія, 2008. 496 с.

9. Про Збройні Сили України: Закон України. *Відомості Верховної Ради України*. 1992. № 9. Ст.108 (зі змінами і доповненнями).

10. Богуцький П.П., Скуріхін С.М. Основи військового права України: курс лекцій. 2-ге вид., перероб. та доп. Одеса: Фенікс, 2011. 343 с.

11. Богуцький П.П. Ознаки та компоненти військового права як комплексної галузі українського права. *Актуальні проблеми держави і права*. – (Національний університет “Одеська юридична академія”). 2005. № 25. С. 151-158.

12. Бойовий статут сухопутних військ ЗСУ: Наказ командуючого сухопутними військами ЗСУ від 29.12.10. № 575. URL: <https://uk.wikipedia.org/wiki>

13. Юридичний словник / за ред. В.М. Бабія, В.М. Корецького, В.В. Цветкова. Київ, 1974. 846 с.

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

УДК 347.193.2:352.075

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

## ТРАНСФОРМАЦІЯ СУСПІЛЬНИХ ВІДНОСИН У ПРОЦЕСІ УТВОРЕННЯ ОБ'ЄДНАНИХ ТЕРИТОРІАЛЬНИХ ГРОМАД

**Анотація.** В даній статті досліджуються питання щодо наявних складностей утворення об'єднаних територіальних громад у процесі децентралізації в Україні, ефективності створення можливостей для об'єднаних територіальних громад у створенні системи надання ними населенню різного роду публічних послуг.; розкриваються наявні законодавчі невирішеності у врегулюванні суспільних відносин в об'єднаних територіальних громадах, напрацьовано відповідні пропозиції щодо врегулювання існуючих проблемних питань у реалізації об'єднаними територіальними громадами своїх повноважень.

**Ключові слова:** законодавство, контроль, повноваження, префекти, спроможні громади, фінансові ресурси.

**Summary.** This article examines the issues the difficulties of forming a united territorial community in the process of decentralization in Ukraine, the effectiveness of creating opportunities for united territorial communities in creating a system of providing them with a variety of public services by such communities, reveals existing legal uncertainties in the regulation of public relations in the united territorial communities, appropriate proposals have been made to address existing issues in the exercise of the powers of the United Territorial Communities.

**Keywords:** legislation, control, powers, prefects, capable communities, financial resources.

**Аннотация.** В данной статье исследуются вопросы об имеющихся сложностях образования объединенных территориальных общин в процессе децентрализации в Украине, эффективности создания возможностей для объединенных территориальных общин в создании системы предоставления ими населению различного рода публичных услуг, раскрываются имеющиеся законодательные нерешенности в урегулировании общественных отношений в объединенных территориальных общинах, наработаны соответствующие предложения по урегулированию существующих проблемных вопросов в реализации объединенными территориальными общинами своих полномочий.

**Ключевые слова:** законодательство, контроль, полномочия, префекты, способные общины, финансовые ресурсы.

**Постановка проблеми.** Утворення об'єднаних територіальних громад (далі – ОТГ) у процесі здійснення децентралізації в Україні є напроцуд актуальним і складним питанням для українського суспільства. Унікальним для зазначеного є те, що утворення ОТГ здійснюється за принципом добровільності, це – з одного боку. А з другого – відчувається наявність значної кількості її противників в особі керівників відповідних населених пунктів. З третього боку – відсутній чіткий сценарій формування ОТГ, а також його альтернативи – виходу із ОТГ. Водночас, у зв'язку з розширенням повноважень ОТГ, дедалі більшої актуальності набуває проблема реалізації державної виконавчої влади на відповідних територіях, оскільки з розширенням повноважень місцевого самоврядування кардинально змінюються функції місцевих органів виконавчої влади і насамперед місцевих державних адміністрацій.

Створення різнобічних можливостей для реалізації громадянами своїх прав та законних інтересів знаходить своє вираження у створенні системи надання різного роду публічних послуг (адміністративних, освітніх, медичних, соціально-культурних тощо). Ці функції мають бути притаманні здебільшого органам місцевого самоврядування і саме під ці послуги вони повинні формувати фінансові ресурси.

**Метою статті** є оцінка питання повноти отримання об'єднаними територіальними громадами необхідних повноважень, наявності належної спроможності та ефективності застосування нових повноважень та існуючих проблем, пов'язаних із даним питанням, напрацювання відповідних пропозиції щодо шляхів їх усунення.

**Виклад основного матеріалу.** Продовження реформи децентралізації в Україні провадиться через об'єднання базових територіальних громад (міст, сіл, селищ) в укрупнені територіальні одиниці – так звані об'єднані територіальні громади. Попередній Уряд визначив підтримку реформи децентралізації в Україні одним з пріоритетних завдань, що сприятиме розвитку місцевого самоуправління і економічного розвитку країни в цілому. Очікувалося, що 2019 рік мав би стати ключовим у питанні формування базового рівня місцевого самоврядування: до кінця 2019 року більшість з існуючих малочисельних місцевих рад мали об'єднатися, а отже стати спроможними перебрати на себе більшість повноважень, належним чином використовувати ресурси і нести відповідальність за свої дії чи бездіяльність перед людьми та державою. Це мало б створити стійке підґрунтя для наступних кроків реформи місцевого самоврядування, а також сприяти прискоренню реформ у сфері охорони здоров'я, освіти, культури, соціальних послуг, енергоефективності та інших секторах.

Певним стимулом для нарощування темпів формування спроможних громад стало нормативно-правове забезпечення добровільного приєднання територіальних громад до вже сформованих ОТГ та певних особливостей такого приєднання. Це стало можливим завдяки Законами України [1; 2]. Перший Закон дозволив за спрощеною процедурою приєднуватися до ОТГ тим громадам, які мають відповідну спільну межу і за перспективним планом формування територій громад області належать до цього об'єднання. Відповідно до Закону, голову ОТГ, до якої приєднується сусідня громада, не переобирають, а вибори депутатів ради ОТГ проводяться лише на приєднаній території. Водночас приєднана громада стає старостинським округом у відповідній ОТГ, а голова приєднаної громади стає старостою і входить до виконавчого комітету ОТГ (за посадою). Як і у випадку добровільного об'єднання громад, ініціатором приєднання можуть бути голова, депутати чи мешканці ОТГ або приєднуваної громади.

Другий же Закон України [2] передбачає можливість утворення об'єднаних територіальних громад, суб'єктом утворення яких є, зокрема, територіальні громади міст обласного значення без зміни меж відповідних районів, а також визначення чіткої послідовності дій в процесі призначення перших місцевих виборів у територіальних громадах, утворених в результаті об'єднання територіальних громад різних районів, та зміни меж таких районів.

Прийнятий через рік Закон України про внесення змін до Закону про добровільне об'єднання територіальних громад від 3 квітня 2018 р. [3], надав спрощену можливість для об'єднання відповідних громад за принципом приєднання територій, що не потребує необхідності проведення перевиборів відповідного міського голови та відповідної міської ради, але передбачає обов'язкове включення голови приєднаної громади до виконавчого комітету міської ради відповідного міста обласного значення. Ухвалення цього Закону України надало відчутний імпульс процесу формування ОТГ. Разом з тим, проблемною позицією цього закону є те, що він юридично позбавляє міські

територіальні громади, які межують з містами обласного значення, можливості такого приєднання.

Саме формат приєднання громад до міст обласного значення відносять до ключових рушіїв добровільного об'єднання громад на новому етапі реформи децентралізації. Старт нового етапу реформи децентралізації відображено у Плані заходів Уряду з реалізації нового етапу реформування місцевого самоврядування та територіальної організації влади в Україні на 2019 – 2021 рр., що було ухвалено відповідним Розпорядженням Кабінету Міністрів України від 23.01.19 р. [4]. Ключовим завданням цього етапу є затвердження нової територіальної основи для діяльності органів влади на рівні громад і районів шляхом фіналізації процесу добровільного об'єднання громад. Суспільний запит на подальше підвищення спроможності громад та політична воля до проведення місцевих виборів 2020 року на новій територіальній основі актуалізують потребу завершити процес формування об'єднаних громад за допомогою додаткових нормативно-правових стимулів. Йдеться про прискорення затвердження перспективних планів ОТГ усіх областей із 100 % покриттям територій; максимальне сприяння добровільному об'єднанню/приєднанню громад, особливо до міст обласного значення; затвердження території громад усіх областей, тобто завершення створення адміністративно-територіальних одиниць базового рівня. Це означає, що впродовж 2019 р. процес об'єднання територіальних громад залишається добровільним, тоді як не виключена можливість застосування адміністративного способу затвердження території громад усіх областей у 2020 році.

Основними завданнями заходів є:

- передача (децентралізація) повноважень виконавчої влади органам місцевого самоврядування та їх розмежування між рівнями і органами за принципом субсидіарності;
- створення незалежної ресурсної бази для здійснення повноважень місцевого самоврядування;
- формування ефективної системи служби в органах місцевого самоврядування та органах виконавчої влади;
- упорядкування системи державного контролю та нагляду за законністю діяльності органів місцевого самоврядування;
- розвиток форм прямого народовладдя: виборів, референдумів;
- удосконалення механізмів координації діяльності центральних та місцевих органів виконавчої влади.

Зазначимо, що згадані заходи потребують подальшого розвитку законодавчої бази. Тому наступним кроком має бути внесення відповідних змін до Конституції України щодо децентралізації, які необхідні для подальшого просування реформи та її завершення. Також існує необхідність у прийнятті ряду важливих законів, таких як:

– ***Про засади адміністративно-територіального устрою України.*** В рамках чинної Конституції України мають визначатися засади, на яких має ґрунтуватися адміністративно-територіальний устрій України, види населених пунктів, систему адміністративно-територіальних одиниць, повноваження органів державної влади та органів місцевого самоврядування з питань адміністративно-територіального устрою, порядок утворення, ліквідації, встановлення і зміни меж адміністративних територіальних одиниць та населених пунктів, ведення Державного реєстру адміністративно-територіальних одиниць та населених пунктів України.

– ***Про внесення змін до Закону України “Про регулювання містобудівної діяльності”.*** Має усунути існуючі недоліки регулювання містобудівної діяльності, унеможливити нецільове використання та розподіл земель.

– *Про службу в органах місцевого самоврядування* (нова редакція). Має забезпечити рівний доступ до служби в ОМС, підвищить престижність служби в ОМС, мотивацію місцевих службовців до розвитку громад та власного розвитку.

– *Щодо державного нагляду за законністю рішень органів місцевого самоврядування*. Україна – єдина європейська країна, де немає системи контролю за рішеннями органів місцевого самоврядування. На сьогодні законодавчо не передбачено нагляду за законністю рішень органів місцевого самоврядування та за дотриманням прав і свобод громадян. Три роки тому попередній механізм, за яким загальний нагляд за рішеннями місцевої влади здійснювала прокуратура, було скасовано. Із того часу органи місцевого самоврядування працюють у певному правовому вакуумі. Введення посади префектів замість голів ОДА передбачене проектом Закону України “Про внесення змін до Конституції України (щодо децентралізації влади)”. Конституційні новели викликали чимало критичних зауважень в експертному середовищі, в представників громадськості та багатьох народних депутатів. Тому великі очікування покладені на профільний закон про префектів, який би мав деталізувати форми та порядок реалізації префектами їхніх повноважень і тим самим розв’язати побоювання.

Планується, що префект має бути представником державної влади, державним службовцем, не належить до політичних посад, не змінюється зі зміною президента чи уряду, не залежить від місцевих політичних еліт. У відносинах з органами місцевого самоврядування (далі – ОМС) префект має мати такі повноваження: наглядає за конституційністю та законністю рішень ОМС; не може оцінювати доцільність та ефективність рішень ОМС; зупиняє дію незаконних актів ОМС і водночас звертається до суду; не ухвалює остаточного рішення про законність актів ОМС, це може вирішувати виключно суд; може порадити місцевій раді привести своє рішення у відповідність до Конституції та законів; оприлюднює повідомлення про зупинку акту ОМС; має менше повноважень, ніж нинішні місцеві держадміністрації.

Передбачається, що префекти діятимуть у кожному районі та в кожній області. В Києва та Севастополя будуть власні префекти. Відповідно до законопроекту, інститут префектів з’являється після набуття чинності змінами до Конституції щодо децентралізації й, відповідно, після ліквідації місцевих держадміністрацій.

Рада Європи постійно наголошує на проблемі відсутності державного нагляду за рішеннями органів місцевого самоврядування в Україні. Професор Страсбурзького університету, експерт Ради Європи Р. Герцог підтримав ідеї та підходи, викладені в розробленому групою експертів новому законопроекті, який би нарешті скоротив кількість контролюючих органів і впорядкував систему державного нагляду за законністю рішень місцевого самоврядування [5].

Європейська сторона сподівається, що переговори щодо нового закону закінчатимуться компромісом й українське законодавство вийде на рівень законодавства розвинутих європейських держав. Роботу органів місцевого самоврядування нарешті буде впорядковано і вони отримають єдину, чітку та прозору систему нагляду. Важливо також, що новий законопроект скасує всі процедури контролю за додержанням законності з боку будь-яких інших органів.

Новий законопроект передбачає, що наглядати за законністю рішень місцевого самоврядування буде лише один орган. Причому він матиме чіткі функції та чітку методику роботи. По суті, це буде орган державної влади, який активно співпрацюватиме з органами місцевого самоврядування. Тобто він захищатиме інтереси держави, але при цьому буде обов’язково враховувати інтереси місцевих органів влади. Річ у тому, що коли останні приймають незаконні рішення, то найчастіше роблять це ненавмисно. Можливо



деякі закони є занадто складними, можливо ще щось. Тож, власне, в особах працівників державного органу нагляду голови громад отримують професійних радників, які сприятимуть тому, щоб усі рішення місцевої влади відповідали законодавству.

У результаті чергові місцеві вибори восени 2020 року мають пройти на новій територіальній основі районів та громад. Повноваження між рівнями управління повинні бути розмежовані за принципом субсидіарності. Мешканці громад мають бути забезпечені механізмами та інструментами впливу на місцеву владу та участі у прийнятті рішень.

У рамках проведення реформи з децентралізації влади на місця передано значні ресурси та повноваження, ефективність використання яких значною мірою залежить від організації контролю за виконанням законів, рішень, розпоряджень та інших документів. Систематичний контроль є необхідною умовою виявлення та усунення недоліків у діяльності органів місцевого самоврядування та причин, що їх породжують. На практиці наслідки такої безконтрольності полягають у тому, що органи місцевого самоврядування часто не виконують своїх обов'язків (наприклад, Шепетівка, Сміла та Славутич невчасно почали опалювальний сезон – за наявності відповідних коштів); як, власне, і законодавство, яке зобов'язує їх вчасно це зробити. Це – порушення ст. 365 Кримінального кодексу України (перевищення влади) [6].

– **Про загальноукраїнський та місцевий референдуми.** Після ухвалення Рішення Конституційним Судом України у 2018 році щодо неконституційності Закону України “Про всеукраїнський референдум” [7], у сфері народовладдя утворилася велика прогалина, як на державному, так і на місцевому рівнях. Місцевий референдум є важливим інститутом безпосередньої демократії, що дозволяє громадянам України, які проживають на території відповідної адміністративно-територіальної одиниці, реалізувати право на прийняття рішень з найважливіших питань місцевого значення.

Право громадян на участь в управлінні місцевими справами ґрунтується на статтях 38, 69 і 70 Конституції України [8]. Зокрема, стаття 38 передбачає право громадян на участь в управлінні державними справами через всеукраїнський та місцевий референдуми, а в статті 69 зазначено, що референдум є волевиявленням народу, поряд з виборами та іншими формами прямої демократії. Місцевий референдум передбачений статтею 7 базового Закону України “Про місцеве самоврядування в Україні” 1997 р. [9] як “форма вирішення територіальною громадою питань місцевого значення шляхом прямого волевиявлення”. У цій статті міститься посилання на інший законодавчий акт для визначення умов і процедури місцевих референдумів.

Активне залучення громадян у процеси прийняття управлінських рішень на місцевому рівні є умовою успішної реалізації політики децентралізації державної влади в Україні, впровадження адміністративної та територіальної реформ, удосконалення вітчизняного інституту місцевого самоврядування.

– **Оновлення законів про місцеві вибори, про місцеве самоврядування** тощо.

Необхідно зазначити, що повноваження органів ОТГ доволі широкі: від розробки стратегії розвитку до організації благоустрою сіл і селищ, які входять до складу ОТГ. Фактично місцева влада починає працювати для мешканців, а не “для галочки”. Мешканців об'єднаних громад вже не відправляють вирішувати питання в район чи область – за все тепер відповідає місцева влада: голова, депутати ради громади та її виконком. Освіта, медицина, адміністративні послуги, дороги, освітлення, водопостачання, сміття, благоустрій, забудова і навіть безпека – компетенція влади об'єднаної громади. Саме влада громади, і більше ніхто, займається вирішенням більшості місцевих питань, має на це кошти і несе за усе відповідальність.

Мешканці об'єднаних громад мають поруч ефективну спроможну владу, яку самі обирають і на діяльність якої можуть впливати. Як наслідок – в містах і селах громади доступніші та якісніші послуги, більш сприятливі умови життя.

Об'єднання не робить громади автоматично заможними. Так, там з'являється більше повноважень і грошей. Але це ще не означає розвиток. Для успіху потрібні лідери, готові діяти рішуче, професіонали, здатні залучити і ефективно використати кошти, керівники, готові нести відповідальність за свою роботу перед людьми і державою.

В процесі об'єднання громад такі місцеві лідери отримують свій шанс: стають головами громад, депутатами, старостами чи громадськими активістами. Для них – це можливість очолити зміни тут і зараз, зробити своє місто чи село кращим, стати частиною успіху країни.

Повноваження, ресурси і відповідальність передаються від центральної влади на місця, бо тільки так можна побудувати міцну державу, стійку до політичних змін всередині та зовнішніх зазіхань.

Рушійною силою в країні стають не політики і чиновники, а сильні заможні громади. Вони долають зневіру людей, бо починають дійсно піклуватися про них: надають якісні та доступні послуги, будують дороги та інфраструктуру, турбуються про безпеку людей, не чекаючи, поки це зробить хтось “згори”. В об'єднаних громадах є на це і повноваження, і кошти. Тому там зростає довіра до влади, підвищується патріотизм, зникає відчуття безпорадності, зростає активність людей.

До початку 2020 року в Україні створено 1009 ОТГ. Загалом же, за затвердженими перспективними планами, має бути створено 1289 ОТГ. Передовими регіонами у процесі створення ОТГ є Волинська обл. (57 % населення); Житомирська обл. (67 %); Сумська обл. (69 %); Тернопільська обл. (60 %). “Пасуть задніх” такі регіони: Дніпропетровська обл. (20 % населення); Закарпатська обл. (19 %); Кіровоградська обл. (17 %); Львівська обл. (13 %); Одеська обл. (15 %); Харківська обл. (14 %).

Перші вибори депутатів сільських, селищної, міських рад ОТГ відповідних сільських, селищного, міських голів, відбулися 22 грудня 2019 року в 86 ОТГ 21 області України – 69 сільських, 16 селищних та однієї міської.

Одним із ефективних механізмів діяльності ОТГ є співробітництво, оскільки міста та села мають низку питань, які складно вирішувати самотійно. Наприклад – збір, утилізація та переробка сміття, забезпечення якісного централізованого водопостачання та водовідведення, ремонт та прибирання доріг, організація пасажирських перевезень, утримання пожежної охорони тощо.

Впоратися з цим легше, якщо співпрацювати – об'єднувати кошти і зусилля з сусідніми громадами, які в цьому теж зацікавлені. Механізм такої міжмуніципальної консолідації передбачений Законом України “Про співробітництво територіальних громад” [10]. З того часу сотні громад через укладання договорів про співпрацю поліпшили якість послуг, що надаються на їхній території. Такими, наприклад, є: Договір про співробітництво територіальних громад у формі створення спільного комунального підприємства (Хмельницька область, Віньковецький район); Договір про співробітництво територіальних громад у формі спільного фінансування (утримання) місцевої пожежної охорони (Хмельницька область, Віньковецький р-н) тощо. Тепер, коли є успішний досвід, цей механізм починає користуватися ще більшою популярністю.

Як свідчить практика, в ході процесу децентралізації спроможні громади отримали більш широкі повноваження, ресурси і відповідальність. Перелік послуг, які можуть надаватися на місцях, постійно розширюється. Мешканці об'єднаних громад очікують від місцевої влади зручних та якісних адміністративних послуг. Саме тому важливо,

щоб кожна об'єднана громада якнайшвидше вирішила, у який спосіб швидко та доступно надавати ці послуги мешканцям.

Очевидно, що в об'єднаних громадах мають бути сучасні Центри надання адміністративних послуг (далі – ЦНАП) – єдине місце (приміщення), де можна отримати найнеобхідніші адміністративні послуги у комфортних умовах. 87 ЦНАП було створено або модернізовано за підтримки Програми “U-LEAD з Європою” [11], завдяки якій 1,2 мільйони мешканців громад та міст України отримали доступ до якісних адміністративних послуг. Так, 26 листопада 2019 р. у Борсуківській сільській ОТГ Тернопільської області відкрився сучасний ЦНАП, а також 5 віддалених робочих місць у с. Борщівка, с. Великі Кусківці, с. Синівці, с. Нападівка та с. Передмірка. Така система надання адмінпослуг в ОТГ була створена на основі договору про міжмуніципальне співробітництво громад. Мешканці громади отримали доступ до 113 послуг в основному ЦНАП і 67 послуг на ВРМ. Громада провела ремонт приміщення та облаштувала його для осіб з інвалідністю, а Програма надала меблі, техніку, програмне забезпечення, а також дитячий куточок для ЦНАП. Всі працівники пройшли тренінги з підвищення кваліфікації, спеціально розроблені українськими, шведськими та естонськими експертами Програми “U-LEAD з Європою”.

Децентралізація владних та фінансових повноважень держави на користь місцевого самоврядування є однією з найбільш визначальних реформ з часів української незалежності. Головним стратегічним завданням модернізації системи державного управління та територіальної організації влади, яка сьогодні здійснюється, є формування ефективного місцевого самоврядування, створення комфортних умов для проживання громадян, надання їм високоякісних та доступних публічних послуг. Досягнення зазначених цілей неможливе без належного рівня економічного розвитку відповідних територій, їх фінансового забезпечення і достатніх джерел для наповнення місцевих бюджетів.

Саме фінансовий аспект є одним із найсуттєвіших, від якого, у великій мірі, залежить успішність функціонування об'єднаних територіальних громад. Наявність економічно активних суб'єктів підприємницької діяльності, достатня кількість кваліфікованих трудових ресурсів, розвинена промислова та соціальна інфраструктура – все це та багато іншого є основою для успішного розвитку громади.

Результатом реформи стало підвищення зацікавленості органів місцевого самоврядування у збільшенні надходжень до місцевих бюджетів, пошуку резервів їх наповнення, покращення ефективності адміністрування податків і зборів. Об'єднані громади показують високі і динамічні темпи приросту власних доходів. У частині використання коштів увага акцентується на необхідності формування найбільш оптимальної структури бюджетних видатків, створенні ефективного не надто чисельного управлінського апарату, здійсненні постійного аналізу витрачання бюджетних коштів і упередженні випадків їх нераціонального витрачання.

Показники виконання місцевих бюджетів відображають загальний соціально-економічний стан відповідної території та її потенціал до сталого розвитку. Наявність достатніх ресурсів у місцевих бюджетах є запорукою того, що територіальна громада має можливість надавати більш якісні та більш різноманітні послуги своїм жителям, реалізовувати соціальні та інфраструктурні проекти, створювати умови для розвитку підприємництва, залучення інвестиційного капіталу, розробляти програми місцевого розвитку та фінансувати інші заходи для всебічного покращення умов проживання жителів громади.

Фінансові ресурси ОТГ складаються із власних доходів і коштів, переданих з державного бюджету. Так власні доходи ОТГ у 2018 році зросли на 62.1 % (до 20.9 млрд. грн.) порівняно з 2017 роком (порівняння здійснено лише щодо 665 ОТГ, які функціонували в 2017 – 2018 роках, виходячи з наявних даних, без ОТГ, які почали функціонувати 2018 року). Власні доходи включають: відрахування від загальнодержавних податків і зборів (податку з доходів фізичних осіб (надходження від якого забезпечують майже 57 % усіх власних доходів ОТГ), акцизів, рентних платежів та ін.), надходження від місцевих податків і зборів (єдиного податку, податку на майно, плати за землю, туристичного збору тощо) та інші надходження (штрафи, кошти від відчуження комунального майна, гранти і т. ін.).

Другу частину доходів ОТГ становлять кошти, які безпосередньо і безоплатно передають об'єднаним територіальним громадам з державного бюджету у вигляді дотацій і субвенцій. Ці кошти йдуть на розвиток ОТГ і фінансування освіти, медицини, соціального захисту. Частка переданих з держбюджету коштів здебільшого коливається в межах 65 – 75 % загальних доходів ОТГ. Основна відмінність дотацій від субвенцій – відсутність обмежень щодо напрямів їх використання, тимчасом як субвенції мають чітко визначені напрями використання. Дотації отримують з держбюджету (базова, стабілізаційна) або передають до держбюджету (реверсна), виходячи з того, наскільки бюджет конкретної ОТГ податкоспроможний порівняно з аналогічним середнім показником за всіма місцевими бюджетами країни. Дотації здебільшого скеровують для фінансування поточних потреб місцевої громади. За даними аналізу фінансових показників діяльності ОТГ за 9 місяців 2018 року, із 665 ОТГ три з чотирьох ОТГ були дотаційними (тобто отримували базову дотацію з держбюджету), 16 % усіх ОТГ – “заможними” (тобто перераховували частину коштів у вигляді реверсної дотації до держбюджету), а в 9 % усіх ОТГ податкоспроможність бюджетів коливалася в межах середньо-українського показника (вони не отримували базової дотації з держбюджету і не перераховували реверсної дотації до держбюджету).

Незважаючи на певні здобутки у питанні здійснення реформи децентралізації, не можна обійти і недоліки та проблеми, які виникли у процесі здійснення реформи. Проблеми, які перешкоджають просуванню реформи децентралізації та розвитку ОТГ, умовно можна поділити на законодавчі та внутрішні. Для формування спроможних громад на рівні можновладців потребують врегулювання (через прийняття відповідних законів) питання, які стосуються: адміністративно-територіального устрою (зокрема порядку утворення та ліквідації адміністративно-територіальних одиниць, встановлення і зміни їх меж тощо); служби в органах місцевого самоврядування (йдеться про надання ОМС більшої автономії у визначенні умов оплати праці для залучення до ОМС професійних кадрів); містобудівної діяльності (в частині просторового планування в ОТГ, зокрема щодо можливості ОТГ розпоряджатися землями, які перебувають на її території, за межами населених пунктів); добровільного об'єднання територіальних громад (зокрема вдосконалення процедури затвердження перспективних планів формування територіальних громад і надання права затверджувати їх виключно КМУ, а не обласним, на рівні яких лобіюють свої інтереси місцеві олігархи, створюючи ОТГ “під себе”).

### **Висновки.**

Серед перешкод розвитку об'єднаних територіальних громад внутрішнього характеру домінують: нестача фінансових ресурсів, брак кваліфікованих кадрів, міграція мешканців ОТГ за її межі, неофіційна зайнятість, низька активність жителів у вирішенні питань функціонування громади та інше.

Як зазначають дослідники та експерти, для повноцінного функціонування місцевого самоврядування в ОТГ необхідно належно вирішити два вкрай важливих і пов'язаних між собою питання. Перше стосується передачі органам місцевого самоврядування належного обсягу повноважень у сфері управління земельними ресурсами, а друге – належні повноваження у сфері планування територій та містобудівної діяльності.

Також слід врахувати недореформований освітній сектор та сектор охорони здоров'я – багато нагальних проблем в цих сферах лягли на плечі ОТГ.

### Використана література

1. Про внесення змін до деяких законодавчих актів України щодо добровільного приєднання територіальних громад: Закон України від 09.02.17 р. № 1851-VIII. *Відомості Верховної Ради України*. 2017. № 13. Ст. 144.

2. Про внесення змін до деяких законодавчих актів України щодо особливостей добровільного об'єднання територіальних громад, розташованих на територіях суміжних районів: Закон України від 14.03.17 р. № 1923-VIII. *Відомості Верховної Ради України*. 2017. № 17. Ст. 203.

3. Про внесення змін до Закону України “Про добровільне об'єднання територіальних громад” щодо добровільного приєднання територіальних громад сіл, селищ до територіальних громад міст республіканського Автономної Республіки Крим, обласного значення: Закон України від 03.04.18 р. № 2379-VIII. *Відомості Верховної Ради України*. 2018. № 20. Ст. 190.

4. Про затвердження плану заходів з реалізації нового етапу реформування місцевого самоврядування та територіальної організації влади в Україні на 2019 – 2021 роки: Розпорядження Кабінету Міністрів України від 23.01.19 р. № 77-р. *Урядовий кур'єр*. 2019. № 34 (20 лютого).

5. Пальчук В. Система державного контролю та нагляду за законністю рішень органів місцевого самоврядування: стан та перспективи. URL: [http://www.nbuviap.gov.ua/index.php?option=com\\_content&view=article&id=4325:sistema-derzhavnogo-kontrolyu-ta-naglyadu-za-zakonnistyu-rishen-organiv-mistseвого-samovryaduvannya-stand-ta-perspektivi&catid=64&Itemid=376](http://www.nbuviap.gov.ua/index.php?option=com_content&view=article&id=4325:sistema-derzhavnogo-kontrolyu-ta-naglyadu-za-zakonnistyu-rishen-organiv-mistseвого-samovryaduvannya-stand-ta-perspektivi&catid=64&Itemid=376) (дата звернення: 30.01.2020).

6. Кримінальний кодекс України: Закон України від 05.04.01 р. № 2341-III. *Відомості Верховної Ради України*. 2001. № 25-26. Ст. 131.

7. Рішення Конституційного Суду України у справі за конституційним поданням 57 народних депутатів України щодо відповідності Конституції України (конституційності) Закону України “Про всеукраїнський референдум” від 26.04.18 р. № 4-п/2018. URL: <https://zakon.rada.gov.ua/laws/show/v004p710-18#n60> (дата звернення: 30.01.2020).

8. Конституція України: Закон України від 28.06.96 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

9. Про місцеве самоврядування в Україні: Закон України від 21.05.97 р. № 280/97-ВР. *Відомості Верховної Ради України*. 1997. № 24. Ст. 170.

10. Про співробітництво територіальних громад: Закон України від 17.06.14 р. № 1508-VII. *Відомості Верховної Ради України*. 2014. № 34. Ст. 1167.

11. Програма U-LEAD. URL: <https://donors.decentralization.gov.ua/project/u-lead>. (дата звернення: 01.02.2020).

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

УДК 342.25 (474.3+477)

ПЕТРИШИН О.О., кандидат юридичних наук,
учений секретар НДІ ДБ та МС НАПрН України.
ORCID: <https://orcid.org/0000-0002-6099-8832>.

РЕФОРМА МІСЦЕВОГО САМОВРЯДУВАННЯ: ДОСВІД ЛАТВІЇ

Анотація. Робота присвячена дослідженню досвіду реформ місцевого самоврядування та адміністративно-територіального устрою в Латвії після відновлення незалежності. В статті систематично та поелементно досліджуються складові частини та напрями реформи: організаційно-структурний аспект; функціональні перетворення; перебудова фреймворку взаємодії з центральною владою; проблеми фінансування повноважень та формування місцевих бюджетів; реформа адміністративно-територіального устрою; проблеми регіонального розвитку; підзвітність та адміністративний нагляд. Підготовлено ряд висновків щодо можливості та доцільності використання досвіду реформ місцевого самоврядування Латвії в контексті завершення реформи децентралізації в Україні та продовження реформ у цьому секторі.

Ключові слова: міське самоврядування, локальна демократія, залучення населення, реформа адміністративно-територіального поділу, регіональний розвиток, Україна, Латвія.

Summary. The paper deals with the experience of reforms of local self-government and administrative and territorial structure in Latvia after its independence was restored. The following components and directions of reform are systematically and elementally studied: organizational and structural aspect; functional transformations; restructuring of the framework of interaction with the central government; problems of financing of powers and formation of local budgets; administrative and territorial division reform; regional development programs; accountability and state supervision. Conclusions have been drawn regarding the feasibility and expediency of using the experience of Latvian local self-government reforms in the context of finalization of the decentralization reform in Ukraine and further reforms in this sector.

Keywords: local government, local democracy, public involvement, reform of administrative and territorial division, regional development, Ukraine, Latvia.

Аннотация. В работе исследован опыт реформ местного самоуправления и административно-территориального устройства в Латвии после восстановления независимости. Систематически и поэлементно исследуются составные части и направления реформы: организационно-структурный аспект; функциональные преобразования; перестройка фреймворка взаимодействия с центральной властью; проблемы финансирования полномочий и формирования местных бюджетов; реформа административно-территориального деления; программы регионального развития; подотчётность и административный надзор. Сделаны выводы касательно возможности и целесообразности использования опыта реформ местного самоуправления Латвии в контексте завершения реформы децентрализации в Украине и продолжения реформ в этом секторе.

Ключевые слова: местное самоуправление, локальная демократия, вовлечение населения, реформа административно-территориального деления, региональное развитие, Украина, Латвия.

Постановка проблеми. Реформа децентралізації, прообраз якої був закладений Концепцією реформування місцевого самоврядування та територіальної організації влади в Україні 2014 року [1], у 2020 році входить до фінального етапу реалізації: внесення змін до Основного Закону в частині адміністративно-територіального устрою; забезпечення механізму державного нагляду за дотриманням відповідності Конституції

та законодавству актів місцевого самоврядування; вирішення питань регламентації та забезпечення власних і делегованих повноважень; побудови ефективних систем регіонального розвитку; ефективізації процесів добровільного об'єднання та укрупнення громад та інших питань.

Досвід реформ країн Балтії в цілому, і зокрема Латвії є важливим та цікавим для України з ряду причин: 1) Латвія та ряд інших країн регіону були одними з перших, що відновили незалежність та дистанціювалися від Радянського Союзу, заявивши про встановлення євроінтеграційного та євроатлантичного курсу; 2) Латвія та Україна мають низку подібних державницьких характеристик (унітарну форму державного устрою, демократичний політичний режим, республіканську, хоча і дещо відмінну, форму правління, схожі моделі адміністративно-територіального поділу тощо); 3) Латвійська Республіка ще у 90-ті роки XX століття пройшла через знайомі нам сьогодні дискурси, наприклад, “Латвія (сьогодні Україна) як міст між Сходом і Заходом”, дискусії щодо нейтралітету держави та інші; 4) До 2004 року в Латвії вже було впроваджено найбільш критичні та ключові реформи місцевого самоврядування, що були продовжені після вступу держави до Європейського Союзу; 5) Після анексії Криму Російською Федерацією в березні 2014 року Україна стала пріоритетним партнером для Латвії щодо забезпечення безпеки в регіоні, що поглибило співробітництво між країнами.

І найголовніше – в Латвії за останні 30 років було проведено низку успішних реформ місцевого самоврядування: розроблено нові закони про місцеве самоврядування та про місцеві вибори; здійснено адміністративно-територіальну реорганізацію; вдосконалено механізми наповнення місцевих бюджетів та місцеві інформаційні (статистичні) системи; створено систему закладів з підготовки кадрів для органів місцевого самоврядування та підвищення їх кваліфікації; переосмислено способи взаємодії між місцевим самоврядуванням та центральними органами виконавчої влади та багато іншого.

Однак, при дослідженні елементів реформ місцевого самоврядування та адміністративно-територіального поділу і їх ефективності слід брати до уваги ряд структурних, масштабних (територія, кількість населення), етнічних, релігійно-культурних та ментальних відмінностей між державами та націями, адже історично Латвія, як і Литовська Республіка, були ідеологічно наближені до держав Західної Європи.

Метою статті є поелементний розгляд та порівняння наступних напрямів реформування місцевого самоврядування в Латвії за період з 1990 по 2020 роки (в контексті завершення реформи децентралізації та АТУ в Україні):

- організаційна структура органів місцевого самоврядування;
- функції та повноваження місцевого самоврядування;
- взаємодія місцевого самоврядування з центральною владою;
- місцеві фінанси;
- адміністративно-територіальна реформа;
- проблеми регіонального розвитку;
- підзвітність та адміністративний нагляд.

Виклад основного матеріалу.

1. Становлення місцевого самоврядування незалежної Латвії.

На початку 2000-х років заслужений латвійський юрист Едвінс Ванагс запропонував наступну періодизацію етапів структурного розвитку місцевого самоврядування незалежної Латвії: 1) перехідний період (1989 – 1992 рр.); 2) прийняття закону “Про місцеві вибори” (січень – травень 1994 р.); 3) місцеве самоврядування за

законом “Про місцеві самоврядування” (з травня 1994 року) [2]. У 2020 році її можна доповнити додатковим періодом (2009 – 2021 рр.), адже реформа адміністративно-територіального устрою, завершена у 2009 році, скоро буде продовжена новою реформою АТУ, що вже закріплена відповідним законом в 2019 році.

Конституція Латвії (*Latvijas Republikas Satversme*) 1922 року, дія якої була в повному обсязі відновлена у 1993 році, надала народу Латвії суверенну владу і передбачила створення Парламенту (*Saeima*), Офісу Президента, Кабінету Міністрів і судів. На відміну від основних законів інших країн регіону (Литви, Естонії) в ній були відсутні будь-які положення щодо місцевого самоврядування, місцевих виборів, комунального майна, локального управління, фінансів тощо.

У 1992 році Парламентом Латвійської Республіки було прийнято резолюцію про підтримку Європейської хартії місцевого самоврядування [3] (частково ратифікована у 1996 році, набула чинності у 1997 р.), а вже у січні 1994 року новостворений Сейм прийняв заснований на положеннях Хартії закон “Про місцеві вибори”. Цим законом закріплювалися принципи таємного голосування, регулярних виборів, обмеження числа представників в окремих місцевих утвореннях, а також правила відбору кандидатів і роль політичних організацій у виборчому процесі [4].

За період з 1991 по 1995 роки було втілено ряд кроків, спрямованих на створення системи, що відповідає потребам різних громад, гарантує цілісність демократичного процесу, а також зміцнює і покращує відносини між державою і місцевим самоврядуванням.

У вересні 1993 року Кабінет Міністрів прийняв Концепцію реформи місцевого самоврядування [5], що створила фундамент для внесення змін до принципів організації і функціонування місцевих органів влади та органів місцевого самоврядування. Цією Концепцією було встановлено принцип, згідно з яким врядування на місцях є незалежним а адміністративні одиниці повинні перебувати під наглядом народно обраних представників.

На основі положень, закріплених в цьому документі, в подальшому було прийнято понад 20 законів, серед яких такі закони: “Про місцеві вибори” від 13 січня 1994 р. [6], “Про місцеві самоврядування” від 19 травня 1994 р. [7], “Про місцеві бюджети” від 29 березня 1995 р. [8], “Про вирівнювання фінансування місцевого самоврядування” від 29 березня 1995 р. [9], “Про адміністративно-територіальну реформу” від 21 жовтня 1998 р. [10]

2. Організаційна структура органів місцевого самоврядування.

Адміністративно-територіальною реформою 2009 року було змінено дворівневу систему поділу муніципалітетів (до реформи округи були муніципалітетами першого рівня, в той час як міста (селища), сільські території та повіти були муніципалітетами другого рівня) на однорівневу. Округи були скасовані, а міста (*pilsētas*), приміські території (*pilsētu lauku teritorijas*), і повіти (*pagasti*) були об’єднані в 110 країв (*novadi*), в той час як 9 великих міст отримали республіканський статус (*republikas pilsētas*).

Відповідно до Закону “Про місцеві самоврядування” (ст. 18 та далі по тексту) внутрішня структура та організація місцевих утворень є однаковою для країв (*novadi*) та міст (*pilsētas*).

Представницьким органом є рада (міська або муніципальна), що складається з депутатів або “радників”. Рада є органом проведення дебатів і прийняття рішень, а її члени обираються громадянами шляхом таємного, загального і прямого голосування, що регламентується вищеназваним Законом “Про місцеві вибори” від 13 січня 1994 року зі змінами та доповненнями. Цей закон також встановлює число депутатів (радників) в

місцевих радах пропорційно до кількості населення, хоча для муніципалітетів і міст застосовуються різні правила.

До компетенції місцевих рад відноситься прийняття найважливіших політичних рішень: місцевого бюджету, внутрішніх підзаконних актів, локального генерального плану та планів економічного розвитку (детальніше у п. 7 роботи), регламентних аспектів та ін. Законом встановлено 27 функцій (або компетенцій) ради, а також будь-які інші компетенції, які можуть бути передбачені галузевим законодавством (ст. 21). Засідання ради є відкритими. Міська рада затверджує свої внутрішні підзаконні акти та регламент. Засідання ради повинні проводитися не рідше одного разу на місяць.

Голова ради вищою виконавчою посадовою особою муніципалітету, його посада є еквівалентною посаді “мера”, хоча в законі такий термін не згадується. Голова обирається членами ради, керує і організовує її роботу (скликає збори, формує порядок денний, вносить пропозиції, організує процес дебатів та ін.). Він також є представником ради у зовнішніх зносинах, особою, що відповідає за виконання судових рішень та має низку інших повноважень (ст. 62 Закону).

Окрім цього, Законом передбачається створення інших органів, таких як постійні комітети або комісії, наприклад, Постійної комісії з питань фінансів, яка може надавати висновки щодо проектів бюджетів та рекомендації щодо управління місцевим майном.

Практична реалізація рішень і впровадження місцевої політики покладається на посадових осіб, обраних або призначених радою та органами місцевого самоврядування (в рамках забезпечення принципу автономності). Наприклад, у муніципалітетах з кількістю населення більше п’яти тисяч обов’язково призначається виконавчий директор (у разі його відсутності його обов’язки виконує голова). Виконавчий директор здійснює ряд виконавчих функцій, наприклад, він має право укладати договори незначної вартості (ст. 69 Закону).

3. Функції та повноваження місцевого самоврядування.

Система місцевого самоврядування та його функції в часи радянської окупації Латвії не є предметом цього дослідження. Разом з тим, необхідно підкреслити формальний характер місцевого самоврядування в цей період. Органи місцевого самоврядування фактично не мали повноважень, а всі важливі рішення до їх впровадження затверджувалися через інститути місцевих комуністичних партій (що відображали політику центральної партії), а інколи через такі інститути на більш високих рівнях. Відтак, навіть якщо формальними виконавцями функцій і були муніципалітети, вони не мали реальних можливостей щодо прийняття рішень. Закріплення функцій та ліквідація фактичного управління з боку держави настало лише після прийняття Закону “Про місцеве самоврядування” у 1994 році та проведення реформи адміністративно-територіального устрою до 2009 року (що включала передачу компетенцій та функцій з округів до найнижчого рівня).

Вищевказаний Закон містить ряд положень, направлених на реалізацію реформи децентралізації, а саме передачі деяких компетенцій та відповідного функціонального навантаження держави на місцевий рівень.

Ст. 6 Закону виділяє: 1) автономні функції, передбачені цим законом; 2) автономні функції, передбачені галузевими правовими актами; 3) делеговані державні адміністративні функції; 4) функції, виконання яких передано органам самоврядування; 5) завдання, покладені на самоврядування державною адміністрацією; 6) автономні функції, які впроваджуються в рамках “добровільних ініціатив”.

На практиці, наведені складні формулювання повноважень можна розділити на дві великі групи – власні та делеговані. Можна також поділити їх на “обов’язкові автономні

функції”, передбачені законами, автономні функції, виконувані в якості добровільних ініціатив, і делеговані функції від імені держави.

До автономних функцій, серед інших, Законом віднесено: соціальне забезпечення; транспорт; місцеві дороги; культуру; утримання громадських служб; дошкільну, початкову та середню освіту; охорону навколишнього середовища та водопостачання; утилізацію відходів; управління комунальними службами та інші (всього 22 пункти). Окрім цього, ст. 17 Закону встановлено перелік додаткових обов’язкових функцій міста-столиці Риги в рамках підтримки діяльності центрального уряду, серед яких: 1) розташування національних урядових установ; 2) прийом іноземних дипломатів; 3) розташування іноземних дипломатичних місій; 4) допомога міжнародним організаціям; 5) підтримка і розвиток інфраструктури державного значення.

4. Взаємодія місцевого самоврядування з центральною владою.

Взаємодія між центральним урядом і органами місцевого самоврядування в Латвії відбувається в межах таких контактних точок: 1) при розробці проектів нормативно-правових актів, що регламентують діяльність місцевого самоврядування; 2) при виділенні щорічних загальних і специфічних грантів (в тому числі щодо реалізації планів регіонального розвитку); 3) при встановленні джерел фінансування для виконання делегованих повноважень; 4) при опрацюванні інших питань, що зачіпають місцеві інтереси [11].

В процесі пошуку оптимальних способів взаємодії протягом 1992-93 років велися тривалі переговори щодо кількості рівнів, необхідних для ефективного функціонування системи місцевого самоврядування. Проміжним результатом переговорів стало продовження дворівневої системи з більш жорстким визначенням ролей для кожного рівня і зменшенням повноважень округів по відношенню до муніципалітетів [12]. Ці принципи знайшли своє відображення в Законі “Про місцеві самоврядування” від 19 травня 1994 року.

У 1996 році центральний уряд підготував пропозицію про скасування районних управлінь і створення територіальних державних адміністрацій. Результатом експерименту стала низка змін до Закону “Про місцеві вибори”, на основі яких в березні 1997 року були обрані тільки ради самоврядувань першого рівня, а не обласні ради. В подальшому ця тенденція не знайшла підтримки, і в листопаді того ж року в Законі “Про місцеві самоврядування” були внесені поправки, що уможливили створення районних рад у складі голів муніципальних рад. Цим радам було доручено виконувати регіональні та функції, делеговані муніципалітетами, а також надавати допомогу в координації надання послуг в сфері освіти, охорони здоров’я, соціального забезпечення і культури [13].

Результати цього експерименту продемонстрували, що таке непряме представництво на обласному рівні не може забезпечити його неупереджене функціонування; кожен представник в першу чергу відстоює інтереси свого муніципалітету, а не району. Окрім цього, відповідно до Закону “Про місцеві самоврядування” в кожному районі і республіканському місті були створені консультативні ради для координації діяльності органів місцевого самоврядування та держави. До складу консультативних рад входили представники муніципальних та обласних органів влади і державних установ. Їх діяльність була неефективною в основному з двох причин: рішення вимагали одноголосної згоди всіх представників і, в кінцевому підсумку, були скоріше рекомендаціями, ніж директивами. Такі ради функціонували з 1994 по 1997 роки, а остаточний кінець подібним експериментам поклала реформа адміністративно-територіального устрою, що завершилася у 2009 повною ліквідацією окружного рівня.

Сьогодні в переговорах з державою інтереси місцевого самоврядування представляє Латвійська асоціація місцевих та регіональних самоврядувань (*Latvijas Pašvaldību savienība*, далі – Асоціація) [14]. За результатами щорічних переговорів між робочими групами, сформованими з представників Асоціації та всіх міністерств (останнім часом – і Парламенту) складаються відповідні документи (протоколи). Зазвичай найбільш гостро при проведенні подібних переговорів постає питання розподілу бюджетних асигнувань.

В рамках Асоціації процес прийняття рішень організовано на кількох рівнях. Вищим органом, який приймає рішення, є Загальні збори членів, що скликаються не рідше одного разу на рік. Зазвичай Загальні збори скликаються спільно з вищим керівним органом Асоціації – Конгресом. У проміжках між засіданнями Конгресу Асоціація управляється Радою, в той час як Панель керує Асоціацією в проміжках між сесіями Ради [15].

Вирішальну роль в розробці політик і підготовці висновків органів місцевого самоврядування відіграють постійні комітети. Наприклад, Комітет з фінансів та економіки, Комітет з освіти та культури, Комітет з соціальних питань і питань охорони здоров'я, Комітет з регіонального розвитку і співпраці та Комітет з народного господарства. Комітети збираються щомісяця для обговорення широкого кола питань. Асоціація відкрита для співпраці і бере участь у вирішенні практично всіх питань, важливих для органів місцевого самоврядування.

Окрім супроводження переговорів, Асоціація є одним із засновників недержавної організації “Латвійський муніципальний навчальний центр” [16], що проводить заходи з підготовки місцевих кадрів та підвищення кваліфікації. Також Асоціація пропонує ряд послуг органам місцевого самоврядування, наприклад: фінансові консультації, розробку моделі фінансування інвестиційних проєктів; формування проєктів для структурних фондів (та фінансування з боку Європейського Союзу); підготовку техніко-економічних обґрунтувань і бізнес-планів; підготовку документації для отримання кредитів тощо.

5. Місцеві фінанси.

Окрім Закону “Про місцеві самоврядування”, основними правовими актами, що регулюють питання фінансування та наповнення місцевих бюджетів є закони “Про бюджети і фінансовий менеджмент” 1994 року [17], “Про бюджети місцевих самоврядувань” 1995 року, “Про вирівнювання фінансів самоврядувань” 2015 року та “Про податки і збори” 1995 року [18].

Основні джерела місцевих доходів формуються за рахунок податкових надходжень, нефіскальних доходів і трансфертів. Механізм встановлення місцевих податків в латвійській моделі замінено на пропорційний розподіл при зборі деяких державних податків. Місцеві органи отримують відсоток (частку) від певних державних податків. Кожна самоврядна одиниця отримує відсоток від загального обсягу зібраних податків на своїй території, до яких належать: прибутковий податок з фізичних осіб (80 %), податок на нерухомість (100 %), податки на лотереї та азартні ігри (25 %), податок на природні ресурси (30 – 100 %).

Крім наведених вище надходжень, муніципалітети та міста можуть збирати інші доходи фіскального характеру, ставку яких вони визначають самостійно, наприклад: послуги, що надаються місцевою адміністрацією; видача офіційних документів і сертифікатів; ведення торгівлі в громадських місцях; розміщення реклами тощо.

Структура доходів місцевого самоврядування за даними 2017 року виглядає наступним чином: 63,5 % формує розподіл податків; 29,4 % бюджетні трансферти; 5,2 % власні доходи; 1,8 % неподаткові доходи; 0,1 % пожертви та 0,1 % фінансова допомога

міжнародних партнерів. За даними Асоціації, тільки 40 % з цих 63,5 % поступає безпосередньо до муніципалітетів, жителі яких створюють ці податки, залишок розподіляється через систему вирівнювання за наведеною вище схемою [19].

Варто окремо відзначити таке джерело фінансування як цільові трансферти з державного бюджету, які надаються для реалізації конкретних функцій (п. 3 роботи). Зазвичай це дотації на оплату праці вчителів, шкільний транспорт, утримання і будівництво доріг і співфінансування проєктів з використанням коштів Європейського Союзу. Органи місцевого самоврядування також мають доступ до фондів ЄС, створених для фінансування проєктів у сферах міського і селищного розвитку, та інших сферах, пов'язаних з муніципальним життям. Але подібні фонди є нестабільними та зазвичай агенції та органи ЄС, такі як Європейський інвестиційний банк, в якості обов'язкових умов вказують співфінансування проєктів, забезпечити яке муніципалітети не мають можливості [20].

Повертаючись до ролі Асоціації у переговорному процесі між місцевим самоврядуванням та центральними органами влади, підкреслюємо, що Кабінет Міністрів за сприяння Асоціації узгоджує з муніципалітетами питання розміру субсидій і цільових дотацій, порядку вирівнювання муніципальних фінансових ресурсів, якщо це не передбачено законом, та джерел фінансування нових автономних функцій, закріплених галузевими законами за місцевим самоврядуванням.

Як і в Литовській Республіці, внаслідок світової економічної кризи 2008 року, латвійські самоврядування сьогодні мають обмежені можливості щодо доступу до ринку запозичень. Вони можуть отримувати довгострокові запозичення тільки для фінансування інвестиційних інфраструктурних проєктів, а не для покриття операційних витрат, а також подавати заявки на отримання короткострокової позики, яка повинна бути повернута до кінця фінансового року. Ситуація загострюється тим, що Латвія не ратифікувала Європейську хартію місцевого самоврядування в повному обсязі та вона не взяла на себе обов'язків щодо імплементації п. 8 ст. 9 цього документу, в якому вказано, що “для цілей здійснення позик інвестиційного капіталу органи місцевого самоврядування мають доступ до національного ринку капіталу в межах закону” [21].

Не допомагає в цій ситуації і досить непростий та бюрократизований механізм отримання таких коштів. Запозичення повинні затверджуватися спеціальною комісією, створеною при Міністерстві фінансів, і проходити через державне казначейство. Відтак, місцевому самоврядуванню не забезпечено доступ до вільних приватних фінансових ринків. Вони можуть подавати документи на отримання кредитів до внутрішніх банків тільки в тому випадку, якщо умови кредитування більш сприятливі, ніж ті, що пропонуються державним казначейством. В цьому випадку для укладення договору також потрібен дозвіл міністра фінансів. Такі запозичення зазвичай не можуть перевищувати 20 % доходів поточного бюджету місцевого самоврядування. Щорічно Законом “Про державний бюджет” встановлюються ліміти для запозичень місцевими органами самоврядування, а також цілі, на які місцеві суб'єкти можуть їх отримувати (що узгоджуються шляхом вже наведеного переговорного процесу між Асоціацією та міністром фінансів).

6. Адміністративно-територіальна реформа.

Адміністративно-територіальна реформа, завершена у 2009 році, основними каталізаторами якої були саме євроінтеграційні прагнення Латвії, була розпочата у 1994 році з прийняття Закону “Про місцеві самоврядування” та здійснювалася в трьох аспектах:

- 1) безпосередньо адміністративно-територіальному (Закон “Про адміністративні території та поселення” 2008 року);
- 2) фінансовому (Закони “Про фінансове вирівнювання ресурсів самоуправління” та “Про бюджети самоуправління” 1995 року.
- 3) юридично-правовому (Закон “Про місцеві самоврядування” 1994 року).

Метою та основними цілями реформи визначалися формування спроможних територій, забезпечення доступу населення до якісних послуг та створення умов для кадрового зростання в самоврядуваннях.

Як і в Україні, реформа адміністративно-територіального устрою в Латвії була більше політичним рішенням, що просувалося від держави до громадян, і мало на меті реформування застарілої радянської системи на основі частково ратифікованої Європейської хартії місцевого самоврядування та підготовку країни до вступу до Європейського Союзу. Процес укрупнення та об’єднання невеликих утворень (повітів) проходив дуже повільно (в тому числі внаслідок відсутності закріплення часових рамок завершення процесу амальгамації), оскільки жителі, з одного боку розуміючи перспективи щодо розвитку, все ж висловлювали побоювання щодо можливої втрати впливу на процес прийняття локальних рішень [22].

Результатом реформи стало створення нових адміністративно-територіальних одиниць – муніципалітетів або країв (*novadi*) з повноцінним місцевим самоуправлінням, а більш дрібні повіти (*pagasti*), що були звичною одиницею для населення до реформи, формально залишились, але втратили власні органи самоврядування.

Такий підхід дозволив уникнути зайвих стресів серед населення, особливо в питаннях укрупнення та злиття невеликих самоврядних одиниць, що є важливим в контексті проведення адміністративно-територіальної реформи та створення ОТГ в Україні. Основною мотивацією до амальгамації невеликих утворень стала значна фінансова підтримка державою подібних ініціатив, окрім додаткової дотації в розмірі 5 % до загального бюджету об’єднаних повітів, кожне об’єднання отримувало 285 тисяч євро в якості разової допомоги, але лише в разі закінчення усіх необхідних процедур до 2009 року (що було регламентовано відповідними поправками до закону).

Таким чином, витративши майже 160 млн. євро на цей проект (та примусово об’єднавши понад 35 одиниць без нарахування дотацій), Латвія змогла в короткі строки провести реформу та покращити матеріальне та інфраструктурне становище нових об’єднань, не зважаючи на те, що в першій версії Закону “Про адміністративно-територіальну реформу” 1998 року не встановлювалися граничні рамки завершення процесу амальгамації.

Результатом реформи стало те, що сьогодні крупні самоуправління та міста республіканського значення мають реальні можливості виконувати більшість повноважень місцевого самоврядування, зазначені в Законі, але все ще існують невеликі самоврядні одиниці (до 1000 населення), що досі не можуть ефективно виконувати свої функції. Для таких випадків передбачалось створення регіонального самоуправління, яке фактично так і було введено.

Як результат, наприкінці 2019 року, не зважаючи на заперечення Асоціації, уряд прийняв концептуальну доповідь Міністерства охорони навколишнього середовища та регіонального розвитку Латвії щодо адміністративно-територіальний поділу, яка передбачає укрупнення існуючих 110 муніципалітетів або країв (*novadi*) до 36. Міністерство буде відповідати за реалізацію реформи [23].

З наукової точки зору такий підхід виглядає обґрунтованим, особливо беручи до уваги співвідношення розміру територій держави – майже 65 тис. кілометрів та кількості

населення – приблизно 2 мільйони. Подальше укрупнення повинно сприяти підвищенню рівня розвитку регіонів (в тому числі за рахунок вирівнювання) та забезпеченню надання послуг населенню відповідно до Європейської хартії місцевого самоврядування.

7. Проблеми регіонального розвитку.

Після відновлення незалежності перед Латвією серед інших постала проблема значної непропорційності потенціалів та розвитку регіонів. Формальне існування місцевого самоврядування та класична для радянського союзу жорстка модель централізації призвела до того, що станом на 2002 рік, 68 % загального обсягу валового внутрішнього продукту вироблялося в столичному регіоні, з яких 58 % – в самому місті Рига.

Перші кроки щодо виправлення ситуації вводилися ще з 1996 року, після прийняття Кабінетом Міністрів проекту концепції “Про стимулювання економіки регіонального розвитку” [24] та розробки єдиної системи калькуляції показників ефективності. На підставі цього проекту у 1998 році парламентом було прийнято Закон “Про розвиток територіального планування”.

До завершення адміністративно-територіальної реформи 2009 року в Латвії політики та плани розвитку регіонів розроблялися на найнижчому (525 повітів), окружному (26 округів) та регіональному (5 планових регіонів) рівнях, перші два з яких є елементами адміністративно-територіального поділу. Лише у 2010 році було розроблено першу загальнонаціональну програму регіонального розвитку “Латвія 2030” [25].

Положення програми були деталізовані в новому законі 2011 року “Про розвиток територіального планування” [26] та ряді актів Кабінету Міністрів щодо планування, будівництва та розвитку земельної інфраструктури. Відповідно до закону було інтегровано механізм довгострокових перспектив для всієї території, встановлені пріоритети, цілі розвитку та більш гнучкі умови планування: 1) можливість розробки плану для всього муніципалітету, а також для окремих його частин (в сільській частині); 2) необов’язковість деталізації планів, що знімає необхідність внесення правок та коректив.

У 2014 році було прийнято Закон “Про землекористування”, що заклав старт земельної реформи, а у 2015 – запущено нову систему територіального планування (Spatial Planning System) [27]. Система передбачала три рівні територіального планування: 1) національний (стратегія Латвія 2030, розвиток об’єктів та територій національного значення, план розвитку приморських територій); 2) регіональний (стратегія та програма розвитку); 3) муніципальний (програми та стратегії сталого розвитку, територіальні плани).

Окрім цього, з 2015 року функціонує інформаційна система територіального планування (Spatial Development Planning Information System). Система забезпечує: 1) супровід процесів розробки документів планування територіального розвитку; 2) розробку, публікацію і ведення даних текстової та графічної частин документів планування територіального розвитку всіх рівнів планування; 3) обмін даними з іншими державними інформаційними системами; 4) механізм долучення до громадських консультацій; 5) отримання електронних послуг [28].

За 5 років функціонування система продемонструвала свою ефективність. Більше того, повне і вчасне інформування місцевого населення та забезпечення можливості прийняття участі в дискусії щодо розвитку регіону проживання створює додатковий механізм залучення громадян до процесів прийняття локальних рішень.

8. Підзвітність та адміністративний нагляд.

В Латвії контроль і нагляд за діяльністю самоврядувань з боку держави здійснюють різні органи і установи. Контроль державних міністерств і відомств за діяльністю

самоврядувань обмежений і строго регламентований законом. Галузевим Міністерством, що відповідає за нагляд і контроль над місцевими самоврядуваннями, є Міністерство охорони навколишнього середовища та регіонального розвитку, що являє собою продукт злиття двох відповідних назві міністерств (далі – Міністерство).

Міністерство здійснює обмежений контроль над органами місцевого самоврядування, адже, відповідно до закону, вони є автономними. Акти індивідуального характеру, прийняті місцевими самоврядуваннями, не можуть бути скасовані або припинені Міністерством. Лише безпосередньо фізична або юридична особа, інтереси якої регламентуються таким рішенням, може подати до адміністративного суду на місцевий орган.

За процедурою, перед затвердженням обов'язкового локального акту органом місцевого самоврядування, разом з пояснювальною запискою він направляється до Міністерства для отримання висновку. Проект аналізується з юридичної точки зору (на предмет компетенції, відповідності його Конституції та законодавству, тощо) протягом 30 днів. Якщо протягом закінчення встановленого строку Міністерство не надає негативного висновку, рішення вважається прийнятим і публікується в офіційному журналі (*Latvijas Vēstnesis*). Якщо Міністерство направляє негативний висновок до відповідної ради, після внесення змін з урахуванням рекомендацій висновку постанова може бути офіційно опублікована. У разі відмови місцевої ради вносити рекомендовані правки, міністр може призупинити дію постанови обґрунтованим розпорядженням, що підлягає публікації в офіційному віснику.

У цьому випадку голова місцевої ради повинен скликати позачергове засідання ради для аналізу та обговорення ситуації, про що міністр повинен бути проінформований. Якщо місцева рада приймає рішення не відкликати або змінювати акт відповідно до рекомендацій міністра, вона зобов'язується подати заяву до Конституційного Суду про скасування дії наказу міністра. У цьому випадку наказ залишається в силі до проголошення рішення суду.

Держава закріплює за собою право відсторонення від посади голови ради муніципалітету у разі регулярного невиконання ним своїх обов'язків або “непослідовності” в його поведінці. Рішення про звільнення голови приймається Міністерством відповідно до процедури зазначеної у розділі XII Закону “Про місцеві самоврядування”. Звільнена особа має право оскаржити таке рішення до компетентного суду.

Окрім цього, держава може розпускати місцеві ради за поданням Міністерства шляхом прийняття відповідного акту Парламентом. Подібні заходи впроваджуються лише у екстрених випадках в разі суворої невідповідності діяльності місцевої ради Конституції та законодавству Латвії, за 25 років з моменту закріплення процедури в Законі “Про місцеві самоврядування” було лише 2 випадки реалізації цієї статті (ст. 92).

Як зазначалося у п.5 цього дослідження, певний обсяг повноважень щодо державного контролю та нагляду лежить на Міністерстві фінансів. Цей орган в установленому порядку стежить за процесом виконання зобов'язань самоврядування, пов'язаних із запозиченнями, і регулярно аналізує фінансове становище самоврядувань, ґрунтуючись на щомісячних звітах. Метою щомісячного фінансового моніторингу з боку Міністерства фінансів є уникнення ризиків щодо фінансової нестабільності місцевих бюджетів.

На тлі світової фінансової кризи 2008 року (та прогнозованої економічної кризи, спричиненої епідемією COVID-19) у Латвії функціонує запобіжний механізм стабілізації місцевих бюджетів, закріплений Законом “Про стабілізацію фінансів місцевих самоврядувань та моніторингу фінансової діяльності місцевих самоврядувань”. Метою

цього закону є регулювання процедур, за допомогою яких здійснюється стабілізація фінансів самоврядувань для безперервного виконання передбачених законом їх функцій у випадках виникнення надзвичайних фінансових труднощів.

Крім державних міністерств, нагляд та контроль за органами місцевого самоврядування здійснюються Бюро державного аудиту (незалежним зовнішнім органом, що в рамках своєї компетенції здійснює нагляд за місцевим самоврядуванням через фінансовий та майновий аудит), Бюро із запобігання корупції та боротьби з нею (антикорупційною державною установою в системі Кабінету Міністрів) і Антимонопольним відомством [29].

Висновки.

Підсумовуючи, зазначаємо, що ряд наведених у роботі проблем, шляхів вирішення, теоретичних концепцій та дійових механізмів можуть і мають бути використані, а також вже в різному обсязі впроваджуються при проведенні реформи децентралізації та адміністративно-територіального устрою в Україні.

В контексті завершального етапу реформи слід відзначити наступні положення та рекомендації: 1) реформа системи органів місцевого самоврядування може бути ефективно проведена без додаткових стресів для населення шляхом зміни статусу окремих утворень без їх ліквідації; 2) чітке та зрозуміле закріплення функцій і компетенцій місцевого самоврядування підсилене забезпеченням автономності та свободи внутрішньої організації може спростити та покращити горизонтальні (міжсамоврядні) та вертикальні (самоврядування – держава) відносини; 3) об'єднання зусиль та підсилення ролі асоціацій органів місцевого самоврядування в забезпеченні діалогу з державою забезпечить дотримання інтересів громадян; 4) перенаправлення державних надходжень на локальний рівень може вирішити проблему недофінансування власних повноважень органів місцевого самоврядування лише в комплексі з введенням систем вирівнювання потенціалу та розвитку регіонів; 5) спрощення системи АТУ, об'єднання та укрупнення адміністративно-територіальних одиниць має забезпечуватися мірами заохочення (дотаціями та виплатами) та примусу (встановлення строків та примусовою амальгамацією); 6) система планування та розвитку регіонів має бути представлена на усіх рівнях, від національного до муніципального, а її забезпечення пакетом сучасних цифрових інструментів має сприяти залученню громадян до процесів прийняття локальних рішень; 7) самоврядність не означає свавілля та безкарність, органи місцевого самоврядування повинні бути підзвітні не лише жителям, але й державі при гарантіях його автономності, відповідності та дотримання принципів *good/collaborative governance*.

Використана література

1. Про схвалення Концепції реформування місцевого самоврядування та територіальної організації влади в Україні. URL: <https://zakon.rada.gov.ua/laws/show/333-2014-%D1%80>
2. Vanags, Edvins Development of Local Government Reforms in Latvia. *Viešoji Politika ir Administravimas*. 2005. № 13. P. 15-24.
3. Європейська хартія місцевого самоврядування. URL: https://zakon.rada.gov.ua/laws/show/994_036
4. Bakken, Larry Baltic Experiences in Local Government: The Historical Development of Local Authority and Local Governance in Lithuania, Latvia, and Estonia. *Hamline Law Review*. Vol. 20. 1997. P. 641-666.
5. Par Pašvaldību reformu koncepciju. URL: <https://likumi.lv/ta/id/234647-par-pasvaldibu-reformu-koncepciju>

6. The City Council and Municipality Council Election Law. URL: https://www.Legislationonline.org/download/id/7704/file/Latvia_Law_City_Council_Municipality_Council_Election_Law_1994_am2013_en.pdf
7. Par pašvaldībām. URL: <https://likumi.lv/ta/id/57255-par-pasvaldibam>
8. Par pašvaldību budžetiem. URL: <https://www.vestnesis.lv/ta/id/34703-par-pasvaldibu-budzetiem>
9. Pašvaldību finanšu izlīdzināšanas likums. URL: <https://likumi.lv/ta/id/274742-pasvaldibu-finansu-izlidzinanas-likums>
10. Administratīvi teritoriālās reformas likums. URL: <https://www.vestnesis.lv/ta/id/51528-administrativi-teritorialas-reformas-likums>
11. Gelazis, Nida. The European Union and the Statelessness Problem in the Baltic States // *European Journal of Migration and Law*. No.6. 2005. P. 225-242.
12. Vagans, Edvins, Dr. Howard R. Balanoff & John F. Lauletta Jr. (1999) After the fall of the soviet union: the changing status of local governments in the republic of Latvia. *International Journal of Public Administration*, 22:1, 135-169, DOI: 10.1080/01900699908525378.
13. Серьогін С.М., Прокопенко Л.Л., Реформування місцевого самоврядування в Литві: досвід для України. *Public Administration Aspects*. ISSN 2311-6420. № 4 (18). 2015. С. 14-21.
14. Latvijas Pašvaldību savienība. URL: <https://www.lps.lv/en>
15. Par LPS. URL: <https://www.lps.lv/lv/par-lps/biedriba>
16. Latvijas pašvaldības mācību centrs. URL: <https://lpmc.lv/par-mums/darbibas-jomas.html>
17. Likums par budžetu un finanšu vadību. URL: <https://likumi.lv/doc.php?id=58057>
18. Par nodokļiem un nodevām. URL: <https://likumi.lv/ta/id/33946-par-nodokliem-un-nodevam>
19. Horvath, Tamas. Decentralization: Experiments and Reforms. URL: http://pdc.ceu.hu/archive/00006917/01/LGI_Decentralization-Experiments-and-Reforms_2000.pdf
20. Diaz-Fuentes, Daniel. The European Investment Bank: Development, Integration, Investment. URL: https://www.academia.edu/36227333/The_European_Investment_Bank_Development_Integration_Investment
21. Local and Regional Democracy in Latvia. URL: <https://rm.coe.int/090000168079c2e8>
22. Administrative territorial structure and reforms in Latvia. URL: <https://www.espon.eu/sites/default/files/attachments/Administrative%20territorial%20structure%20and%20reforms%20in%20Latvia%20by%20Aivars%20Draudins%2C%20Latvia.pdf>
23. Government approves continuing territorial reform. URL: <https://eng.lsm.lv/article/politics/politics/government-approves-continuing-territorial-reform.a332295>
24. Latvijas reģionālā attīstība: stāvoklis, jēdzieni, darbības virzieni. URL: <https://www.vestnesis.lv/ta/id/36743>
25. Raugze, Ilona. Regional development challenges in Latvia towards 2020. URL: <https://nkutvikling.custompublish.com/getfile.php/1802993.1169.xuavpfascc/Regional+development+challenges+in+Latvia+-+Ilona+Raugze.pdf>
26. Teritorijas attīstības plānošanas likums. URL: <https://likumi.lv/ta/id/238807-teritorijas-attistibas-planosanas-likums>
27. Spatial Planning in Latvia 1994 – 2018. URL: <https://www.espon.eu/sites/default/files/attachments/Inguna%20Urtane%20-%20ESPON%20Latvia.pdf>
28. Teritorijas attīstības plānošanas informācijas sistēma. URL: <https://tapis.gov.lv>
29. The Latvian competition authority imposes interim measures suspending concession agreements concluded between a municipality and two waste management companies. URL: <https://www.concurrences.com/en/bulletin/news-issues/september-2019/the-latvian-competition-authority-imposes-interim-measures-suspending>

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

УДК 342.7

**ГОЛОВКО О.М.**, кандидат юридичних наук, старший науковий співробітник  
НДІ інформатики і права НАПрН України,  
старший викладач кафедри публічного права  
НТУУ “КПІ імені Ігоря Сікорського”.  
**ДУБЕНЕЦЬ А.С.**, студентка факультету соціології і права,  
НТУУ “КПІ ім. Ігоря Сікорського”.

## РОЛЬ ЦИФРОВІЗАЦІЇ ДЕРЖАВНИХ ПОСЛУГ У ПРАВОВІДНОСИНАХ З ІНОЗЕМНИМ ЕЛЕМЕНТОМ

**Анотація.** У статті проаналізовано роль та перспективи цифровізації державних послуг у контексті наявності іноземного елемента в житті України з огляду на процес європейської інтеграції нашої держави, досліджено досвід європейських країн у питанні електронного урядування.

**Ключові слова:** цифровізація державних послуг, євроінтеграція, електронне урядування.

**Summary.** This article analyzes the role and perspectives of digitalization of public services in the context of the presence of foreign elements in the life of Ukraine with regard to the process of European integration, European countries' experience in e-governance is explored.

**Keywords:** digitalization of public services, European integration, e-government.

**Аннотация.** В статье проанализирована роль и перспективы цифровизации государственных услуг в контексте наличия иностранного элемента в жизни Украины, с учетом процесса европейской интеграции нашего государства, исследован опыт европейских стран в вопросе электронного управления.

**Ключевые слова:** цифровизация государственных услуг, евроинтеграция, электронное управление.

**Постановка проблеми.** Процес невідпинної цифрової трансформації політичної, економічної, соціальної, культурної сфер життя суспільства свідчить про розвиток глобального цифрового простору, який являє собою рушійну силу побудови інформаційного суспільства та суспільного прогресу. Цифровий сектор економіки України набуває поступової динаміки, адже активне залучення населення у сферу використання цифрових технологій, безпосередньо детермінує стрімке поширення електронної комерції, популяризацію ведення бізнесу через он-лайн платформи, створення інноваційного програмного забезпечення. Зростання значення цифрових комунікацій поступово охоплює не тільки сторону корпоративного або приватного життя особи, але й знаходить своє відображення у взаємодії з державною та муніципальною владою.

В умовах інтеграції України в Європейське співтовариство, питання функціонування електронних сервісів із надання публічних послуг набуває актуальності значення, оскільки зважаючи на реалізацію ЄС цифрової стратегії та досвід впровадження таких систем країнами Європи, зокрема Нідерландами, Данією, Фінляндією, Швецією, свідчить про широкий спектр переваг такої моделі здійснення адміністративної діяльності [4, с. 2].

**Результати аналізу наукових публікацій.** Питаннями дослідження регулювання відносин з іноземним елементом займалися Гожій І.О., Чубарев В.Л. та ін. Розвиток цифровізації, електронного урядування в Україні здійснювали такі вчені, як Погорецька Н.В., Карпенко О.В., Чукут С.А. Проте роль цифровізації державних послуг

у контексті регулювання відносин за участю іноземного елемента в житті України, адже покращення інвестиційного клімату, продовжує бути одним із потенційних чинників розвитку сфери економіки.

**Метою статті** є визначення особливостей правового регулювання суспільних відносин у сфері надання публічних послуг при використанні цифрових технологій.

**Виклад основного матеріалу.** Одним із ключових напрямків діяльності органів державної влади є надання публічних послуг. Так, зокрема Карпенко О.В. під публічними послугами розуміє всі види діяльності органів державної влади та органів місцевого самоврядування, які здійснюються в інтересах як окремого громадянина, так і суспільства, надання яких зумовлене повноваженнями конкретного органу влади, до компетенції якого вони належать [6].

Сучасна парадигма публічного управління передбачає запровадження нових механізмів та підходів, які б сприяли розвитку “партнерської” взаємодії між владою та громадськістю. Суттєву роль у даному питанні відіграє зникнення комунікативних бар’єрів, що виявляється в утвердженні суспільно орієнтовних акцентів при здійсненні державно-владних повноважень публічною владою, публічні звітування перед громадськістю щодо підсумків своєї роботи за певний період, функціонування при державних органах консультативно-дорадчих, забезпечення зворотнього зв’язку.

Саме реалізація комунікаційної стратегії сприяє підвищенню прозорості, відкритості, ефективності органів державної влади. Питання надання публічних послуг відіграє у даному процесі особливу роль, оскільки підвищення їх якості безпосередньо пов’язане із ступенем реалізованості суспільних інтересів тобто результативністю діяльності, що досягається шляхом правової визначеності, забезпечення загального доступу на єдиних засадах.

Особливістю надання публічних послуг в останні роки стала їх “цифровізація”. Квінтесенція розуміння цифровізації є доволі багатогранною. Обраний вектор поєднує у собі використання цифрових технологій для збору, аналізу даних з метою отримання релевантної та структурованої інформації, а також багатоканальне інформування та залучення громадян, електронну ідентифікацію, вільне поширення, використання та розповсюдження відкритих державних даних [2].

Так, Президент Єврокомісії Урсула фон дер Ляєн, у Політичних рекомендаціях Єврокомісії 2019 – 2024 року наголошує, що “цифрові технології, особливо штучний інтелект, змінюють світ з небаченою швидкістю, і їх використання допоможе знайти рішення суспільних проблем від здоров’я до сільського господарства, від безпеки до виробництва” [3, с. 13].

В умовах цифровізації вагому роль відіграє впровадження електронного урядування, що являє собою основний спосіб організації державної влади за допомогою інформаційний мереж. Концепція “електронного урядування” набула значного поширення як на території американського континенту, так і країн західної Європи.

Відстеження прогресу держав-членів ЄС у сфері цифрової конкурентоспроможності стало можливим у зв’язку із запровадженням Європейською Комісією “Індексу цифрової економіки та суспільства”, який базується на таких критеріях:

- інтегрованість цифрових технологій;
- надання державних послуг через інформаційно-телекомунікаційні технології;
- поширеність серед населення застосування он-лайн-сервісів з отриманням послуг [4].

Найвищий показник в імплементації державних послуг зафіксовано у Фінляндії, Естонії, Нідерландах, Іспанії.

Згідно з дослідженнями ООН, викладеними у “United Nations E-Government Survey 2018”, спостерігається позитивна динаміка серед 193 досліджуваних країн світу до зростання рівня розвитку е-уряду. До групи з дуже високим індексом розвитку електронного урядування в 2018 р. віднесено 40 країн; 71 країну – до групи з високим індексом розвитку електронного урядування; 66 країн – з середнім індексом та 16 країн – до групи з низьким [12].

Тенденції розвитку електронного самоврядування простежуються на трьох рівнях:

- міжвідомчому – при взаємодії органів державної влади між собою з метою оптимізації функціонування адміністративного апарату;
- приватному – при партнерстві влади та суб'єктів підприємництва задля скорочення державних витрат за рахунок використання технології аутсорсингу та створення прозорої системи державних закупівель;
- громадському – при співробітництві громадськості з публічною владою з метою залучення громадян до прийняття рішень органами влади, подолання бюрократизованості адміністративної діяльності, побудова електронної демократії.

Доцільно зауважити, що, як вказує Чукут С.А., електронна демократія є вагомим складовою електронного урядування, адже її головною метою є задоволення потреб громадян, досягнення суспільних цінностей шляхом використання переваг інформаційного суспільства, подолання таких негативних явищ як корупція, формалізація сучасного управлінського процесу [9, с. 122].

Сучасний стан цифрових змін у сфері урядування в Україні перебуває на перших етапах активного впровадження, адже імплементація електронного урядування в Україні забезпечує втілення положень Угоди про асоціацію України та ЄС, зокрема у частині співробітництва в галузі електронної торгівлі, регулювання електронно-комунікаційних послуг, відносин з бізнес-спільнотою.

Сталий розвиток цифрового простору в Україні здійснюється під впливом інвестиційної діяльності провідних країн світу, іноземних компаній, зацікавлених у підвищенні рівня технічного розвитку країни та темпів структурної перебудови економіки.

Оцінка перспектив покращення інвестиційного клімату в країні вимагає вдосконалення нормативного регулювання правових відносин приватного характеру, розробки нових підходів щодо формування механізму залучення інвестицій. Враховуючи дані Держстату України надходження прямих інвестицій (акціонерного капіталу) в Україну за січень – вересень 2019 склали 1 668,3 млрд. долларів США. Окрім того, приплив прямих іноземних інвестицій в Україну у 2019 році склав 2,5 млрд. долл. США. Станом на 01 жовтня 2019 року найвагоміші обсяги надходжень прямих інвестицій були спрямовані до підприємств промисловості – 33,3 % та установ та організацій, що здійснюють оптову та роздрібну торгівлю, ремонт автотранспортних засобів і мотоциклів – 16,6 % [10].

Функціонування іноземних юридичних осіб в Україні безпосередньо вимагає екстериторіального визнання їх правосуб'єктності на основі внутрішніх норм країни перебування та міжнародних договорів, укладених між Україною та іноземною державою [11].

Встановлення наявності підстав, або обмеження щодо здійснення підприємницької діяльності, а також порядок здійснення реєстрації, отримання ліцензій визначається законодавством України. У даному контексті, запровадження можливості електронної реєстрації іноземної юридичної особи, дозволило не тільки спростити процедуру, але і

дистанційно здійснювати підготовку, редагування або доукомплектування необхідних документів без географічних обмежень.

Регламентація правового статусу юридичних осіб, здійснюється за допомогою норм міжнародного приватного права, які передбачають визначення меж правосуб'єктності, тобто обсягу її правоздатності та дієздатності на основі особистого закону юридичної особи та державної приналежності, що відіграє ключову роль у встановленні ознак юридичної особи або навпаки – їх відсутності, організаційно-правової структури.

Досліджуючи питання реєстрації іноземних юридичних осіб в Україні Чубарев В.Л., звертає увагу на випадки, коли згідно з національним правом юридичної особи не вимагається реєстрація у торговому реєстрі, однак за українським законодавством передбачено надання витягу із торгового реєстру у разі реєстрації представництв іноземних суб'єктів господарської діяльності в Україні [11, с. 109].

З цього приводу Дзера О.В. зазначає, що французькі юридичні особи, які вчиняють операції з нерухомістю, землепорядкуванням, а також компанії для спільної професійної діяльності (цивільні професійні компанії ревізорів тощо) не зобов'язані поширювати (публікувати) про себе відомості, зокрема реєструвати їх у торговому реєстрі [12].

Окрім цього, стаття 25 Закону України “Про міжнародне приватне право” визначає особистим законом юридичної особи право держави місцезнаходження юридичної особи (її створення), а у випадку відсутності таких умов – право держави, у якій знаходиться виконавчий орган управління юридичної особи [1].

Існування різних підходів до сутності особистого закону юридичної особи, як зазначає Погорецька Н.В., негативно впливає на розвиток міжнародних економічних відносин, оскільки може призвести до виникнення проблеми “подвійної національності” юридичної особи, подвійного оподаткування або відсутності податкового доміліцію. При цьому, виникає необхідність врахування існуючих офшорних зон та практику виведення підприємства з-під юрисдикції держави, а тому доцільним є встановлення та застосування критерію контролю до компаній, які зареєстровані в офшорній зоні [13, с. 104].

Отже, правове регулювання функціонування представництв, філій, дочірніх компаній іноземної юридичної особи спрямоване на створення сприятливих умов для здійснення підприємницької діяльності, адже принципова зміна умов щодо реєстрації, а саме зменшення строку на її здійснення та адміністративного збору, що передбачені Постановою Кабінету Міністрів України від 23.10.19 р. № 893, є одним із факторів позитивного впливу на бізнес-клімат в Україні.

Водночас, впровадження цифрових технологій у наданні публічних послуг іноземним компаніям допоможе вирішити ряд питань, пов'язаних з підготовкою та поданням документів до уповноваженого органу, скоротить час на їх обробку, мінімізує розбіжності або помилки в документах. Важливим кроком у цьому питанні стало запровадження Державною фіскальною службою оплати податків, зборів та ЄСВ он-лайн, і хоча наразі система перебуває у пілотній експлуатації, такі реформи свідчать про прагнення України відповідати європейським стандартам у сфері надання цифрових послуг.

Разом з тим, в умовах підвищення інтенсивності глобальних міграційних процесів актуальності набуває дослідження перспектив цифровізації державних послуг, які надаються у процесі регулювання суспільних відносин приватного характеру, ускладнених іноземним елементом.

Так, за даними Державної міграційної служби, станом на 1 вересня 2019 року в Україні на обліку перебуває 280872 іноземці, які проживають на підставі посвідки на постійне проживання та 114394 іноземців, які проживають в Україні на підставі посвідки на тимчасове проживання. Водночас, за даними колишнього міністра соціальної політики Рєви А.О., майже 3 міл. 200 тисяч українців працюють за кордоном на постійній основі, однак ця цифра може зростати і до 6 – 7 міл., оскільки трудова міграція має і сезонний характер [16].

Однак, однією з найбільш колізійних сфер у міжнародному приватному праві є спадкові відносини, адже зв'язок особи з декількома правопорядками призводить до ускладнення вирішення таких питань як: визначення кола спадкоємців, вимог до форми заповіту, складу спадкового майна, дійсності заповіту тощо.

Наприклад, законодавство деяких країн, зокрема Німеччини, передбачає право укладання спільних заповітів подружжя, а в Англії, США – вільних заповітів. На противагу цьому, законодавство Італії, Польщі визнає заповіт тільки як односторонній акт. Натомість, Французький цивільний кодекс прямо забороняє спільні і взаємні заповіти [7, с. 289].

Вимоги до змісту заповіту теж мають особливості. У деяких країнах передбачається можливість призначити спадкоємців та вирішення питань щодо розпорядження майном. Законодавство інших країн, крім розпоряджень майнового характеру і визначення кола спадкоємців, допускає у заповіті також положення щодо визнання позашлюбної дитини, призначення неповнолітньому опікуна, призначення виконавця заповіту [7, с. 290].

В умовах переходу в Україні до надання цифровізованих державних послуг, вважаємо за необхідне створення окремого розділу в Єдиному реєстрі заповітів та спадкових прав, до якого будуть вноситися справи, пов'язані з регулюванням спадкових відносин за участю іноземного елемента. При цьому необхідно урахувати особливості формування та описування таких справ, зумовлені їх змістом. Такий підхід обумовлений плюралізмом правопорядків, які можуть бути застосовані для регламентації спадкових відносин і буде сприяти належній систематизації.

Не менш вагому роль при врегулюванні відносин за участю іноземного елемента відіграють справи про міжнародне усиновлення, адже загальнонаціональним пріоритетом у політиці держави є охорона та захист прав, інтересів дитини, забезпечення реалізації прав дитина на життя, охорону здоров'я, освіту, соціальний захист тощо [5]. Вдосконалення інституту усиновлення в Україні детерміновано щорічним зростанням кількості дітей, які залишилися без батьківської турботи. Статистика Міністерства соціальної політики України вказує, що станом на 31 грудня 2018 року в Україні на обліку дітей-сиріт та дітей, позбавлених батьківського піклування перебувало 70491 дитина, із них 22126 дітей-сиріт та 48365 дітей, позбавлених батьківського піклування. Наведені дані не можуть не приголомшувати. Слід зазначити, що з кожним роком увага суспільства до вирішення питання забезпечення дітей зростає. Так, згідно стану на 31 березня 2018 року в Україні функціонувало 1039 дитячих будинків сімейного типу, в яких виховувалося 6929 дітей та 3646 прийомних сімей, в яких виховувалося 6863 дитини [17].

Міжнародне усиновлення відіграє помітну роль у наданні дітям-сиротам та дітям, які залишились без батьківського піклування, благополучних умов виховання в сім'ї. Особливістю колізійного регулювання відносин з усиновлення в Україні є застосування кумуляції, тобто одночасного використання права різних держав, з якими зазначені відносини мають юридичний зв'язок [8, с. 2]. Відповідно до частини 1 статті 69 Закону

України “Про міжнародне приватне право” – “усиновлення та його скасування регулюються особистим законом дитини та особистим законом усиновлювача. Якщо усиновлювач – подружжя, яке не має спільного особистого закону, то застосовується право, що визначає правові наслідки шлюбу” [1].

Проаналізувавши дану норму, ми можемо стверджувати, що вона є двосторонньою колізійною нормою, оскільки вона прямо не визначає право якої держави повинно бути застосоване, однак формулює загальний принцип, за допомогою якого можна обрати право. Разом з тим, колізійні норми щодо усиновлення містяться у договорах про правову допомогу: договори з Польщею, Грузією, КНДР, В'єтнамом.

У деяких договорах передбачено, що у справах про усиновлення чи його скасування особами з різним громадянством компетентними є установи тієї договірної держави на території якої подружжя має чи мало спільне місце проживання або місцеперебування (ст. 33 Договору з Албанією, ст. 26 – з Алжиром) [7, с. 269].

Процедура усиновлення здійснюється відповідно до Порядку провадження діяльності з усиновлення та здійснення нагляду за дотриманням прав усиновлених дітей від 08 жовтня 2008 року, затвердженого Постановою Кабінету Міністрів України. Порядок передбачає, що громадяни України, які проживають за межами України, іноземці, які бажають усиновити дитину, беруться на облік Державним департаментом усиновлення та захисту прав дитини, попередньо подавши справу із необхідними документами, перелік яких встановлений абзацом п'ятим пункту 91 Порядку. Важливим є те, що стати усиновлювачем особа може лише після отримання рішення про усиновленням дитини.

З цього приводу Гожій І.О. зазначає, що процедура міждержавного усиновлення в Україні складна і досить громіздка, що насамперед пояснюється необхідністю одночасного використання правових приписів країн, з якими суб'єкти правовідносин мають юридичний зв'язок [8, с. 4].

Погоджуючись із думкою автора, ми вважаємо, що цифровізація державних послуг при здійсненні процедури міждержавного усиновлення виявляється у доцільності оцифровування та переведення в електронний вигляд окремих документів та дій, наприклад, можливість електронної реєстрації для подачі документів до уповноваженого органу або отримання запрошення на співбесіду для ознайомлення з інформацією про дітей, які можуть бути усиновленими. На нашу думку, створення такої альтернативи детерміновано тим, що здійснення процедури міждержавного усиновлення дитини займає досить тривалий час та вимагає виконання ряду дій особисто усиновлювачем або через представника: подання справи до Міністерства соціальної політики, знайомство та встановлення контакту з дитиною, участь у судовому засіданні, і тому переведення деяких “проміжних” етапів усиновлення в електронну форму забезпечить встановлення відповідності процедури викликам сучасності та сприятиме розвантаженню, оптимізації роботи уповноважених органів.

### **Висновки.**

Узагальнюючи вищезазначене, вважаємо, що роль цифровізації державних послуг є вагомим у кожній сфері діяльності держави, адже цифрові технології відкривають унікальні перспективи розвитку і створюють рівні можливості для кожного у доступі до інформації та знань. Вони забезпечують ефективну взаємодію органів державної влади та громадян, результатом чого є оптимізація механізму участі громадськості в державному управлінні та перехід на якісно новий рівень “діалогу” – електронну демократію, підвищення прозорості, відкритості органів державної влади. Будучи потужною рушійною силою, цифрові технології стимулюють впровадження інноваційних підходів у

виробництві та створенні цифрових інфраструктур, залученні іноземних інвестицій, налагодженні міжнародного співробітництва, тим самим забезпечуючи економічний прогрес України.

### Використана література

1. Про міжнародне приватне право: Закон України від 23.06.05 р. № 2709-IV. *Відомості Верховної Ради України*. 2005. № 32. С. 422.
2. Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та затвердження плану заходів щодо її реалізації: Закон України від 17.01.18 р. № 67-р. URL: <https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80> (дата звернення: 01.02.2020).
3. Political guidelines for the next European Commission 2019 – 2024 by Ursula von der Leyen URL: [https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf) (дата звернення: 03.02.2020).
4. The Digital Economy and Society Index (DESI). URL: <https://ec.europa.eu/digital-single-market/en/desi> (дата звернення: 04.02.2020).
5. Про охорону дитинства: Закон України від 26.04.01 р. № 2402. *Відомості Верховної Ради України*. 2001. № 30. С. 142.
6. Карпенко О.В. Управлінські послуги в Україні: механізми надання органами влади. Київ: АМУ, 2014. 408 с.
7. Федіняк Г.С., Федіняк Л.С. Міжнародне приватне право: підручник. 4-е вид., перероб. і допов. Київ: Атіка, 2009. 500 с.
8. Гожій І.О. Деякі питання колізійного регулювання міждержавного усиновлення. *Політологія. Соціологія. Право*. – (Вісник НТУУ “КПІ ім. Ігоря Сікорського”). Вип. 1/2 (29/30) 2016.
9. Чукут С.А. Кращі європейські практики впровадження електронного урядування: досвід Данії. *Інвестиції: практика та досвід*. 2016. № 24. С. 141.
10. Інвестиції зовнішньоекономічної діяльності. – (Державна служба статистики). URL: [http://ukrstat.gov.ua/metaopus/2019/2\\_05\\_03\\_01\\_2019.htm](http://ukrstat.gov.ua/metaopus/2019/2_05_03_01_2019.htm) (дата звернення: 18.02.2020).
11. Чубарєв В.Л. Статус юридичної особи в міжнародному приватному праві. *Вісник Академії адвокатури України*. 2009. № 3(16). С. 104-109.
12. United Nations E-Government Survey 2018. URL: <https://publicadministration.un.org/en/research/un-e-government-surveys> (дата звернення: 18.02.2020).
13. Цивільне право України: підруч. У 2 кн. Кн. 2. 2-е вид. / О.В. Дзера, Д.В. Боброва, А.С. Довгерт та ін.; за ред. О.В. Дзери, Н.С. Кузнецової. – (Київський Нац. ун-т ім. Т. Шевченка). Київ: Юрінком Інтер, 2001, 780 с. URL: [https://pidruchniki.com/1566072147024/pravo/klasifikatsiya\\_yuridichnih\\_osib\\_pravi\\_zarubizhnih\\_derzhav#98](https://pidruchniki.com/1566072147024/pravo/klasifikatsiya_yuridichnih_osib_pravi_zarubizhnih_derzhav#98) (дата звернення: 18.02.2020).
14. Погорецька Н.В. Національність юридичної особи. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2013. № 3. С. 100-107.
15. Рева А.О. Трудова міграція – катастрофа для України? DSNEWS. URL: [https://www.youtube.com/watch?v=P8j6Hpa\\_9Cg](https://www.youtube.com/watch?v=P8j6Hpa_9Cg) (дата звернення: 23.02.2020).
16. Моніторинг міграційної ситуації та змін у сфері управління міграцією та кордонами. URL: [https://dmsu.gov.ua/assets/files/migprocess/zvit\\_vypusk\\_29.pdf](https://dmsu.gov.ua/assets/files/migprocess/zvit_vypusk_29.pdf) (дата звернення: 23.02.2020).
17. Мета деінституалізації – реалізація права кожної дитини на сім'ю. URL: <https://www.msp.gov.ua/news/15560.html> (дата звернення: 23.02.2020).

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


УДК 343.2:342.77(477)“17/20”

ВРОНСЬКА Т.В., доктор історичних наук, с.н.с., головний науковий співробітник НДІ інформатики і права НАПрН України.
ORCID: <https://orcid.org/0000-0001-7762-5461>.

БЕЛАНЮК М.В., кандидат юридичних наук, учений секретарь НДІ інформатики і права НАПрН України.
ORCID: <https://orcid.org/0000-0002-3083-1732>.

ОСОБЛИВОСТІ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЦИВІЛЬНОГО НАСЕЛЕННЯ В УМОВАХ ВОЄННОГО/НАДЗВИЧАЙНОГО СТАНУ (на українських землях XVII – початок XX ст.)

Анотація. У статті аналізуються історико-правові засади запровадження особливих правових режимів (воєнного та надзвичайного станів) і спричинене ними розширення юрисдикції військових судів за рахунок цивільного населення, а також своєрідність каральних практик у цих умовах. Трансформація надзвичайного законодавства, пов'язана з появою регулярного війська в умовах збройних конфліктів, і специфіка підсудності досліджується у широких хронологічних межах – від Козацької доби до початку XX ст., коли остаточно викристалізувалася система регламентних нормативних документів, які фіксували межі кримінальної та адміністративної відповідальності цивільних осіб під час запровадження особливих правових режимів.

Ключові слова: воєнний стан, надзвичайний стан, військовий суд, кримінальна відповідальність, цивільне населення.

Summary: The article analyzes the historical and legal basis for the introduction of special legal regimes (martial and emergency law) and the resulting expansion of the jurisdiction of military courts at the expense of the civilian population, as well as the peculiarity of punitive practice in these conditions. The transformation of emergency legislation related to the emergence of a regular army in armed conflict and the specifics of jurisdiction are studied in a wide chronological range – from the Cossack era to the beginning of the twentieth century, when the system of regulatory documents was established fixing the boundaries of criminal and administrative liability of civilians during the introduction of special legal regimes.

Keywords: martial law, state of emergency, military court, criminal liability, civilian population.

Аннотация: В статье проанализированы историко-правовые основы введения специальных правовых режимов (военного и чрезвычайного положения) и вытекающее из этого расширение юрисдикции военных судов за счет гражданского населения, а также своеобразность карательной практики в этих условиях. Трансформация чрезвычайного законодательства, связанного с появлением регулярной армии в условиях вооруженных конфликтов, и специфика юрисдикции исследуются в широком хронологическом диапазоне – от казацкой эпохи до начала XX века, когда окончательно определилась система регламентных нормативных документов, фиксировавших границы уголовной и административной ответственности гражданских лиц в период введения специальных правовых режимов.

Ключевые слова: военное положение, чрезвычайное положение, военный суд, уголовная ответственность, гражданское население.

Постановка проблеми. Останнім часом з'являється дедалі більше наукових праць, де так чи інакше зачіпаються питання функціонування військових судів в умовах особливих правових режимів. Перші праці, де мимохідь висвітлювалася згадана проблема, з'явилися ще на початку XX ст. Найглибший аналіз надзвичайних правових

режимів в Російській імперії, зокрема й розширення юрисдикції військової Феміди, у 1908 р. здійснив російський правник і публіцист В. Гессен [1]. Він зміг зазирнути за лаштунки творення надзвичайного законодавства, висвітлив світовий досвід, схаактеризував політико-правові, соціальні наслідки невинправданої пролонгації адміністративно-поліцейського режиму. Пізніше правовий режим воєнного стану в певних хронологічних межах з акцентом на інституційні аспекти розглядали й інші науковці [2], а серед них і українські: Вовк Ю., Рогожин О., Рум'янцеv В., Тимошук О., Ярмиш А. та ін. [3].

Серед багатьох окремо варто виділити ґрунтовну колективну працю “Судова влада в Україні...” (2014 р.) [4], в якій українські науковці здійснили глибокий історико-правовий екскурс у товщу століть, а також зосередили свою увагу на юрисдикції військових судів у різні періоди державності й бездержавності України.

Навіть дуже стислий історіографічний огляд досліджуваної теми дає змогу переконатися у тому, що в історико-правовій науці питання підсудності цивільних осіб розглядалося лише фрагментарно. Окреме студіювання згаданої тематики у широких хронологічних межах не здійснювалося. Лише в окремих публікаціях, більшість з яких має доволі чіткі хронологічні обмеження, побіжно висвітлюються ці аспекти.

Вивчення історичного досвіду, як позитивного, так і негативного, зокрема й у сфері військового судочинства, компетенція якого поширювалася на цивільних осіб, має теоретико-пізнавальне та практичне значення в період судової реформи в Україні. В сучасній гарячій полеміці навколо проблеми відновлення системи військової юстиції мають висловитися представники історико-правової науки. Їх завдання – аналіз минулого, зокрема, практики судочинства у часи запровадження особливих правових режимів стосовно цивільних осіб. Адже цілком очевидно, що концепція судової реформи має враховувати не лише сучасний європейський та світовий досвід, а й надбання та прорахунки власних шляхів розвитку.

Метою статті є визначення особливостей компетенції військової юстиції стосовно цивільних осіб у часи запровадження надзвичайного та воєнного стану від найдавніших часів до встановлення радянської влади на українських землях.

Завдання статті передбачає виокремити з-поміж інших аспектів функціонування військової юрисдикції проблему розширення підсудності, що супроводжувалося підвищенням рівня суворості каральних санкцій стосовно цивільного населення.

Виклад основного матеріалу. Аналіз правозастосовної практики в умовах запровадження особливих правових режимів, зокрема і воєнного стану, доречно розглядати, звернувшись до нормативно-правових актів минулих століть.

Підвалини військового судочинства, фокусованого на цивільне населення, почали закладатися ще у часи Київської Русі. В “Руській правді”, першому збірнику давньоруського права, були зафіксовані санкції за повстання проти князя, перехід на бік ворога. Справи обвинувачених у згаданих злочинах, які не позиціонувалися як військові, а належали до категорії державних посадовців, хоча й не виділених в окрему групу, перебували у компетенції князівського суду [5, с. 175]. Пізніше – у першому Литовському статуті (Зводі законів 1529 р.), чинному на українських землях, до якого окрім цивільного, кримінального та інших входили і положення військового права, “за бунт, зраду, недбале несення служби” (тут і далі курсив наш. – Авт.) тощо передбачалася смертна кара [6, с. 23]. У другому Литовському статуті (1566 р.) у 29 статутах розділу 2 “Про оборону...”, окрім передумов запровадження воєнного стану, перелічувалися злочини (зрада, самовільне залишення поля бою, неявка до війська тощо), за які передбачалося покарання за законами надзвичайного часу [7, с. 135].

У системі судочинства Запорозької Січі, яка, не маючи писаного кодифікованого законодавства, спиралася на давні козацькі традиції та звичаєве право, важко виокремити особливості покарання пересічних осіб. Це стосується і періоду національної революції (1648 – 1676 рр.). У ході еволюції січової громади відбувалася кристалізація козацького права. Якісно новий його рівень пов'язаний із вступом запорожців на державну службу. Відтоді почалося формування своєрідного синтезу норм військового права козацтва з офіційним, яке увібрало в себе досвід попередніх часів [8]. У працях українських дослідників знаходимо інформацію про те, що козацьке право передбачало покарання за ухилення від виконання військового обов'язку чи порушення правил його виконання (дезертирство), яке поширювалося як на козаків, так і на тих людей (цивільних), що мешкали за межами Запорозжя в територіальних одиницях Січі – “паланках” [9]. Все це фактично було спричинено життям в умовах перманентного воєнного стану. А відтак військові суди в Запорозькій Січі, з певними застереженнями, можна вважати, прообразом/прототипом окремого (спеціального) виду судочинства з доволі широкими повноваженнями.

Як зауважується у виданні “Судова влада в Україні...”, з посиланням на праці С. Слабченка та Д. Яворницького, у другій половині XVII – XVIII ст.ст. у Новій Запорозькій Січі “судова влада загалом не була відокремлена від військово-адміністративної”. Військовий суддя розглядав як цивільні, так і військові справи, хоча затвердження остаточних ухвал належало до прерогативи кошового отамана. У згаданому дослідженні також наголошується, що о тій порі підсудність справ чітко не визначалася. Тому за таких обставин важко стверджувати про наявність чітко визначеної ієрархії судових органів, проте беззаперечною була вищість “суду Коша” у всіх його формах [10, с. 134, 143].

Абсолютно очевидно, що у своєрідній судовій системі Запорозької Січі, організація якої мала мілітарний характер, домінувала військова складова. Непідсудного простору в тамтешній державній вертикалі тоді не існувало.

У часи, коли українські землі входили до складу Австрійської та Російської імперій, військове судочинство, а відтак і його компетенція стосовно цивільного населення, регулювалося законодавством згаданих держав.

У XVII – XVIII ст. на західноукраїнських землях, інкорпорованих до Габсбурзької монархії (спочатку всі колишні угорські землі, зокрема й українське Закарпаття, від 1772 р. – Східна Галичина, дещо пізніше – Буковина, західна Галичина – *Авт.*), судова влада, зокрема і компетенція військових судів, регламентувалася окремими законами. У 1854 р. були створені військові суди, які розглядали справи військових на підставі Кримінального кодексу 1768 р. [10, с. 259, 304]. У цей час, як і у наступні роки, виокремити юрисдикцію військових судів стосовно цивільних осіб доволі складно. Щоправда, кримінальним кодексом 1787 р., передбачалася смертна кара [повішання] для всіх без винятку мешканців, “якщо винний вчинив замах, що підлягає військовому закону” [11].

На українських землях, які наприкінці XVIII – на початку XIX ст.ст. (внаслідок трьох поділів Польщі, російсько-турецьких війн, ліквідації Гетьманщини і Запорозької Січі) увійшли до складу Російської імперії¹, було поширено загальноімперський адміністративний устрій та законодавство.

¹ У Підросійській Україні на початку XIX ст. проживало 8,2 млн осіб, станом на середину XIX ст. – 20 млн осіб.

Принагідно слід зазначити, що ще за часів правління Петра I *“Воїнський артикул”* і розділи *“Воїнського статуту”* (1716 р.), які вважаються першими військово-кримінальними та військово-судовими (процесуальними) кодексами, що мали о тій порі найвищу юридичну силу, поширювалися не лише на військовослужбовців, а й решту громадян, які проживали на території всієї централізованої держави [12].

Перші законодавчі акти, які регламентували юрисдикцію військової Феміди стосовно підданих, зокрема на українських землях, з'явилися у другій половині XIX ст. Принагідно слід зазначити, що після скасування у 1861 р. кріпацтва пішли у небуття панські суди поміщиків, становий характер селянського суду та юридична відособленість селянства. Спочатку це були розрізнені закони, які ухвалювалися вищою владою Росії в умовах наростання суспільно-політичних антагонізмів, селянських заворушень, терактів проти високопосадовців. Імператори вдавалися до кроків, які, на їх переконання, мали б стабілізувати ситуацію.

Приміром, 5 серпня 1861 р. вийшло схвалене Олександром II положення *“Про правила на випадок оголошення будь-яких місцевостей західних губерній на воєнному стані”* [13, с. 51]. Генерал-губернаторам, більшість з яких мали вищий військовий чин, було дозволено дискретно оголошувати згаданий особливий правовий режим у підвладних губерніях, де не лише чиновники військових і поліцейських відомств, а й цивільне населення переходило під юрисдикцію військових судів. Особи, обвинувачені у зраді, бунті, непокорі військовому та цивільному начальству або агітації (підбурюванні) інших громадян на непокору владі, а також у насильстві, розбої, убивствах, грабунках і підпалах, підлягали військовому суду на підставі чинних законів (польових військово-кримінальних законів: *“Польове кримінальне уложення”* та *“Статут польового судочинства”*), які діяли лише в умовах воєнного стану. 31 серпня 1861 р. київському військовому, подільському й волинському генерал-губернаторові також надавалося право притягувати до відповідальності винних у заворушеннях в оголошених на воєнному стані місцевостях. Згаданих осіб приписувалося судити за законами воєнного часу, а вироки виконувати негайно [13, с. 52].

У наступні роки верховна влада імперії декілька разів запроваджувала воєнний стан у місцевостях, де активізувалися національно-визвольні рухи проти російського панування. Тривала робота з укладання й удосконалення правової бази, яка мала регламентувати порядок притягнення підданих до відповідальності за військово-кримінальним законодавством. За імператорськими указами, у місцевостях, оголошених на воєнному стані, будь-які судові справи цивільних осіб обов'язково переходили до компетенції військових судів² [14]. Принагідно слід наголосити, що окремі злочини, справи щодо яких розглядалися згаданими спеціальними судами, не мали чіткого

² Законодавство Російської імперії постійно вдосконалювалося. Так, у 1864 р. було розпочато роботу зі створення нового *“Воинского устава о наказаниях”*. Вже у 1867 р. було завершено роботу над його Загальною частиною й у цьому ж році її введено в дію. У 1868 р. було введено в дію й Особливу частину цього статуту. Проте у 1874 р. було прийнято новий статут про загальний військовий обов'язок, що поставило вимогу перегляду та погодження з ним *“Воинского устава о наказаниях”* 1867 – 1868 рр. У результаті цієї роботи в 1875 р. був прийнятий новий *“Воинский устав о наказаниях”*. Він ретельно регулював усі можливі засоби охорони військового правопорядку й згодом став основою для розробки чинних у XX ст. на території України військово-кримінальних законів. У 1913 р. *“Воинский устав о наказаниях”* було видано в новій редакції, потім законами від 14 листопада 1914 р. і 12 січня 1916 р. до нього було внесено багато змін. [Романовський Я., Хлопецький О. Історія формування та розвитку військового судочинства на території України. Журнал *“Схід”* № 7 (91)].

закріплення у законі, а визначалися щоразу у випадку оголошення особливого правового режиму.

Під час російсько-турецької війни 1877 р. воєнний стан було оголошено у Бессарабській губернії, приморських повітах Херсонщини та Таврії [15]. Встановлювався особливий порядок підсудності для тих російських підданих, які мешкали на теренах Одеського й Кавказького військових округів, оголошених на воєнному стані. Військовому командуванню згаданих округів надавалося право на власний розсуд передавати до військових судів справи цивільних осіб для розгляду й покарання за законами воєнного часу за такі злочини, як навмисне вбивство, зґвалтування, розбій, пограбування, підпал чи “потоплення” чужого майна [13, с. 53].

1 липня того ж року такий же порядок підсудності поширили на кілька інших регіонів. При цьому збільшився перелік злочинів, кваліфікованих як “найважчі” (напад на вартового чи військовий караул, збройний спротив караулу, навмисне убивство вартового). Право передавати до військового суду делегувалося головнокомандувачам за умов, коли “вони вважали це необхідним” [16].

Указом від 8 квітня 1879 р. “Про порядок процедури розгляду справ осіб цивільного відомства, які передаються до військового суду...” встановлювалися правила, за якими мало здійснюватися судочинство у воєнний час [17] (зафіксовані у V розділі Військово-судового статуту зводу військових постанов 1869 р., кн. XXIV. – Авт.).

Трохи більше, ніж за два роки, з огляду на наростання нестабільності (внутрішньої та зовнішньої), спричиненої убивством Олександра II, 14 серпня 1881 р., було затверджено надважливе, базове урядове положення “Про заходи для збереження державної безпеки і громадського спокою” [18, с. 263]. Ухвалений як тимчасовий, цей документ замінив собою цілу низку розрізнених актів, ухвалених раніше і залишався чинним аж до революції 1917 р. Відповідно до нього у будь-якій місцевості за ініціативою міністра внутрішніх справ, схваленою комітетом міністрів і узгодженою з імператором, міг запроваджуватися не лише воєнний, а й винятковий стан – у формі “посиленої” або “надзвичайної” охорони.

В місцевостях, оголошених у стані *посиленої охорони*, надзвичайні права, зокрема й ухвалення рішень про спрощене судочинство стосовно цивільних осіб, делегувалися вищому місцевому керівництву (генерал-губернаторам, губернаторам, градоначальникам). Справи громадян, обвинувачених у державних злочинах, передавалися до компетенції військових судів. Аналогічні правила діяли і у разі запровадження режиму *надзвичайної охорони*. Втім, генерал-губернатори, яких іменували вже “головноначальниками”, отримували ширші права – аналогічні повноваженням, що мали головнокомандувачі армій у воєнний час. Окрім іншого, вони могли передавати військовому суду справи осіб, які вчинили “злочини відомого роду” (так в оригіналі – Авт.) [18, с. 264]. На свідоме вживання такого розпливчатого формулювання звернув увагу у своїй праці В. Гессен, який зауважував, що не лише визначення “громадський порядок та спокій”, а й щойно згадане, є надто широкими. Їх можна трактувати на власний розсуд. Що, власне, й робили генерал-губернатори, зловживаючи наданими їм повноваженнями. Вони часто-густо передавали справи до військових судів, які застосовували до цивільних осіб покарання у вигляді смертної кари. Згаданий вище російський правник зауважував: “З найсуворішої міри політичної відплати смертна кара перетворюється на покарання, яке призначається, хоча й у винятковому порядку, але за загальні злочини (убивство, грабіж, зґвалтування, розбій, підпал...)..., які ніякого політичного характеру не мають. ...Таким чином життя цивільних осіб опиняється не в руках суду, а в руках адміністративної влади”. І далі,

узагальнюючи свої критичні висновки щодо безпідставності надзорських заходів стосовно цивільного населення в умовах запровадження стану надзвичайної охорони, В. Гессен, використовуючи народну мудрість та свою красномовність, зауважував: “[Прислів’я] Коли горить хата, б’ють шибки”, – не відповідає умовам російської дійсності. Будинок не горить, його мешканці мирно сплять, а шибки все одно б’ють. Отже, – продовжував він, – смішно дивуватися тому, що ми хворі; варто дивуватися тому, що ми живемо” [1].

4 вересня 1881 р. уряд визначив регіони імперії, де запроваджувався режим посиленої охорони. До таких місцевостей потрапили: Харківська, Полтавська, Чернігівська, Київська, Волинська, Подільська, Херсонська губернії, Сімферопольський, Євпаторійський, Ялтинський, Феодосійський, Перекопський повіти, а також міста Бердянськ Таврійської, Маріуполь Катеринославської губерній, Одеське, Таганрозьке, Керч-Єнікальське градоначальства [19].

Невдовзі Положення “Про заходи для збереження державної безпеки і громадського спокою” було поширене на третину всього населення Російської імперії.

Удосконалення законодавства про особливі правові режими тривало й надалі. 18 червня 1892 р. було видано “Правила про місцевості, оголошені на воєнному стані” [20] – документ, який до вже регламентованих режимів посиленої та надзвичайної охорони додавав третій вид – воєнний стан. В окремому розділі цього документа регламентувався порядок спрощеного судочинства для цивільних осіб (з передачею під юрисдикцію військових судів) та, відповідно, підвищений рівень відповідальності за скоєння злочинів, визнаних особливо небезпечними (“бунт проти верховної влади”, “державна зрада”, умисне нищення або пошкодження запасів продовольства, фуражу, водогонів, мостів, доріг, переправ, засобів зв’язку, напад на військовиків тощо). Окрім цього, представники влади мали право на власний розсуд передавати на розгляд військового суду справи про інші злочини, вчинені цивільними особами, але з наступним затвердженням вироків військових судів. Розгляд згаданих справ під час дії воєнного стану доручався імперським військовим судам відповідно до чинного законодавства Росії [20].

У перші роки ХХ ст. у деяких місцевостях Російської імперії, зокрема і на українських землях, воєнний, а не надзвичайний/винятковий, стан оголошувався безпідставно – задля утримання “спокою” всередині держави. Такий особливий правовий режим, як і стан облоги, оголошений у час відсутності збройного конфлікту, іменувався фіктивним. В. Гессен, наводячи у своїй праці приклади безпідставної заміни диктатури цивільної на військову (а відтак і припинення дії Положення 1881 р. із заміною його на “Правила...” 1892 р.)³, наголошував, що надмірне розширення юрисдикції військових судів за рахунок цивільних осіб у таких умовах є безглуздом і не виправданим [1].

Принагідно цей же знаний фахівець у галузі адміністративного права здійснював концептуально важливий порівняльний аналіз надзвичайного законодавства інших держав, підкреслюючи, що воно поділяється на дві категорії: воєнної і цивільної диктатури. І разом з тим наголошував, що в Російській імперії особливий правовий режим одночасно мав ознаки обох диктатур (змішаний характер).

³ У 1905 – 1907 рр. фіктивний воєнний стан запроваджувався імператорськими розпорядженнями в Одесі, Харкові, Херсоні, Кременчуці, разом з усіма повітами, в Казатині, Сарнах та ін. станціях Південно-Західної залізниці та інших місцевостях України.

Звертаючись до досвіду європейських держав XIX ст., зокрема й проблеми зміни підсудності цивільних осіб, В. Гессен зауважував, що, приміром, Англія, Голландія і Австрія не вдавалася до такої практики навіть в умовах воєнного стану. Тим часом в Італії, де надзвичайний чи воєнний стан не був регламентований законодавством, військова юстиція набувала ширших повноважень, ніж де інде, зокрема і за рахунок розширення юрисдикції військових судів. А ось Франція в історії функціонування особливих правових режимів займала особливе місце. Хоча б з огляду на те, що саме надзвичайне законодавство цієї держави, зокрема і закон про воєнний стан (і облоги), ухвалений 8 липня 1791 р., стало прообразом, зразком для наслідування й запозичення інших країн [1]. У цій державі, як згодом і в Російській імперії, уряд мав право запроваджувати згаданий особливий правовий режим у вигляді воєнної диктатури як у випадку зовнішньої агресії, так і у разі внутрішніх заворушень. Щоправда, цивільній владі залишали окремі функції на розсуд військових. Вище керівництво останніх зосереджувало в своїх руках надзвичайні повноваження поліцейського характеру. Окрім іншого, воно отримувало право видаляти “підозрілих” осіб з місця постійного проживання. Злочини та будь-які інші дії *“проти безпеки республіки, конституції, порядку і громадського спокою незалежно від статусу обвинуваченого та співучасників передавалися на розгляд військових судів”*. Зміна підсудності цивільних осіб здійснювалася за наказом командувача дивізії. Разом з тим, військові суди мали право застосовувати стосовно згаданої категорії громадян лише каральні санкції, передбачені кримінальним *“уложенням”* та іншими законами військового права [1]. У Німеччині, як і у Франції, у разі оголошення стану облоги влада переходила до військових. Статті конституції, які гарантували відповідні громадянські свободи призупинялися, а злочини (державна зрада, убивства, спротив владі тощо), вчинені цивільними особами, передавали на розгляд військових судів, які, на відміну від французьких, складалися не лише з військових (двоє з п’яти суддів були цивільними). Значно суворішими були й санкції. За державну зраду винних позбавляли життя.

Узагальнюючи досвід інших держав, В. Гессен зауважував, що розширення повноважень військових судів у репресивній сфері може мати місце лише у випадку крайньої необхідності. До зловживання подібною практикою – ставився вкрай негативно. *“Заміна звичайних судів військовими трибуналами... аналогічна збройній боротьбі з внутрішнім ворогом замість зосередження на ворогах зовнішніх. Військове право може застосовуватися лише на театрі воєнних дій під час іноземного нашествя або громадянської війни, коли суди закриті і цивільна влада de facto позбавлена можливості функціонувати”*, – наголошував він [1].

Після початку першої російської революції влада імперії вкотре схилилася до рішення перекласти судочинство стосовно цивільних громадян на інституції військової Феміди. Підготовка нової редакції профільних законодавчих актів упродовж 1905 – 1906 рр. розгорталася у надрах спеціально створеної комісії⁴. Серед інших, лунали думки щодо недоцільності розширення компетенції військових судів, зокрема й передачі до них справ, фігуранти яких обвинувачуються у злочинах, за котрі не передбачено

⁴ Вперше питання щодо удосконалення чинного законодавства, зокрема й того, що регламентувало особливі правові режими, було ініційоване указом 12 грудня 1904 р. Упорядкування відповідного законопроекту спочатку було покладено на т.зв. особливу нараду, згодом – на спеціальну міжвідомчу комісію, очолювану заступником міністра внутрішніх справ О.О. Макаровим (розстріляного більшовиками у 1919 р. – *Авт.*). Проект нового законодавчого акту, який регламентував винятковий стан розглядався Державною Думою 2 і 4 скликання, але так і не був ухвалений у вигляді остаточного закону.

найсуворішого покарання – смертної кари. На переконання юристів, навіть в умовах воєнного стану пересічні громадяни мають поставати перед звичайними судами, а військовій юстиції належить “опікуватися” тими цивільними особами, які обвинувачуються у збройному спротиві владі, нападі на чинів війська чи поліції, убивстві, нанесенні важких фізичних каліцтв; підпалах, грабунках тощо. Особливий наголос робився на тому, що передача згаданих справ до військових судів має відбуватися не за розсудом тих чи інших посадовців, зокрема й губернаторів, а винятково за чинним законодавством [1]. Проект нового законодавчого акту, який регламентував винятковий стан, розглядався Державною Думою, але так і не був ухвалений у вигляді остаточного закону.

Проте, 19 серпня 1906 р. з метою боротьби з революційним рухом і стабілізації внутрішньополітичної ситуації в Російській імперії⁵ було ухвалене тимчасове Положення Ради Міністрів, згідно з яким тимчасові військово-польові суди, які могли створюватися на вимогу генерал-губернаторів і військового командування у місцевостях, де запроваджувався режим надзвичайної охорони або воєнний стан. Ці інституції – швидкого судочинства чинили “правосуддя” за законодавством воєнного часу. Процедурні питання реалізовувалися у закритому режимі упродовж однієї доби, а вирок оскарженню не підлягав. Упродовж 1906 – 1907 рр. такі суди були створені у переважній більшості губерній Російської імперії [21]. Підсудність військово-польовим судам у Положенні чітко не визначалася. Зафіксовані у документі підстави передачі генерал-губернаторами або іншими уповноваженими особами справ пересічних громадян до згаданих інституцій виглядали доволі розпливчатыми. Змінювати підсудність можна було “у тих випадках, коли вчинене особою цивільного відомства злочинне діяння є настільки очевидним, що немає необхідності в його розслідуванні”. Ця теза, як слушно зауважували і тогочасні і сучасні правники, видається надзвичайно хиткою, оскільки рішення про передачу тієї чи іншої справи до військово-польового суду цілком залежало від думки відповідних посадовців. Відтак створювалися передумови до суб’єктивізму й зловживань [22]. Засуджені до смертної кари люди не могли розраховувати й на помилування імператора не тільки через стислі терміни виконання вироку, а й тому, що губернаторам та командувачам військ, округів давалася вказівка про заборону передавати телеграми про помилування.

Закон про військово-польові суди втратив силу 20 квітня 1907 р., хоча Положення про ці інституції стосовно військових залишалося чинним. Розгляд справ цивільних осіб за згаданими злочинами, вчиненими у місцевостях, оголошених на воєнному стані, посиленої чи надзвичайної охорони, передалися до військово-окружних судів⁶.

Автори видання “Судова влада...” подають статистику розгляду справ цивільних осіб військовими судами в порядку надзвичайної підсудності. Більшість з них мали

⁵ Безпосереднім приводом для ухвалення рішення про створення військово-польових судів став замах, скоєний 12 серпня 1906 р. у Зимовому палаці в Петербурзі, на колишнього міністра внутрішніх справ, голову Ради Міністрів Росії П. Столипіна. Того дня загинуло 27 чоловік, 32 отримали поранення, серед них і його діти. Сам Столипін не постраждав. Проте вислів “мене вб’ють, і вб’ють члени охоранки” багато в чому став пророчим [В.П. Даниленко. Вбивство Столипіна: офіційна версія і архівні документи. *Архіви України*. 2011. № 2 – 3. С. 195-199. URL: <http://dspace.nbuv.gov.ua/handle/123456789/30903>]. Через п’ять років – 18 вересні 1911 р. у Києві внаслідок теракту він пішов з життя.

⁶ Військово-окружні суди в Російській імперії, створені відповідно до військово-судового статуту 1876 р. Функціонували у кожному військовому окрузі, залежно від часу запровадження там чинності згаданого статуту.

політичне забарвлення. Якщо у 1902 – 1904 рр. до військового суду було віддано 74 цивільні особи, то в 1905 і 1906 рр. – відповідно 308 і 4698. У 1907 р. було засуджено 4335 осіб, у 1908 р. – 7016, у 1909 р. – 5400, – зазначається в праці. І далі наголошується: Загалом з червня 1907 р. до липня 1914 р. через військово-окружні суди пройшло понад 21 тис. цивільних осіб – учасників революційного руху. Вироки військових судів характеризувалися винятковою суворістю, а часто – і відвертою жорстокістю. Приміром, за 168 справами стосовно цивільних осіб, переданими у 1906 – 1907 рр. до Київського військово-окружного суду В.О. Сухомлиновим – командувачем військами Київського військового округу і за сумісництвом генерал-губернатором Київської, Подільської і Волинської губерній, 157 осіб було засуджено до смертної кари і 146 – до каторги. Військово-окружні суди держави у 1908 – 1909 рр. засудили до смерті близько 40 % загальної кількості цивільних осіб, які пройшли через ці інституції [10].

Тим часом на українських землях, що входили до складу Австро-Угорщини, чинними залишалися правові норми та судова система Австрійської імперії, уніфіковані судовою реформою у другій половині XIX ст. Судові справи щодо військовослужбовців на території Галичини в цей же період вирішувалися окремими судами трьох інстанцій: військовий суд, вищий військовий суд і Верховний військовий трибунал. Достеменною інформації щодо особливостей підсудності цивільних осіб згаданим спеціальним інституціям допоки виявити не вдалося.

Ще до офіційного оголошення Першої світової війни – 20 липня 1914 р. воєнний стан було запроваджено й на окремих українських територіях⁷, які входили до складу Російської імперії. Там набули чинності *“Правила про місцевості, оголошені на воєнному стані”* від 18 червня 1892 р. 23 липня 1914 р. головнокомандувач військ Південно-Західного фронту М. Іванов, який одночасно обіймав посаду командувача Київського військового округу, посилаючись на указ імператора, власним наказом оголосив до відома й неухильного виконання положення про управління у воєнний час на підлеглих йому територіях. Ішлося й про зміни у судочинстві стосовно цивільних осіб. Найперше й суворіше карали учасників *“бунтів”* проти верховної влади, осіб, котрі знищували або завдавали шкоди шляхам, що мали стратегічне значення, а також зрадників. Із метою прискорення судової процедури запроваджувалися військово-польові суди для покарання тих військовослужбовців, *“учинення якими злочинного діяння”* було *“настільки очевидним”*, що не потребувало розслідування. Військово-польовий суд засновувався за наказом військових начальників і складався з голови та чотирьох офіцерів, які прослужили в армії не менше чотирьох років. Розгляд справ розпочинався негайно і тривав упродовж двох діб. Того ж 20 липня 1914 р. спеціальним указом *“Про затвердження тимчасового положення про військову цензуру”* запроваджувалася кримінальна відповідальність для тих, хто розголошував інформацію про обороноздатність держави. Такі вчинки кваліфікувалися як *“зрада”* і *“шпиунство”* [23].

Одним із наслідків Першої світової війни стала перемога в Росії Лютневої демократичної революції 1917 р., яка поклала край існуванню Російської імперії та створила сприятливі умови для піднесення національно-визвольних рухів, зокрема і на українських землях. У Києві на початку березня 1917 р. було створено національний

⁷ Воєнний стан було оголошено у Холмській, Волинській, Подільській, Бессарабській, Київській, Харківській, Таврійській губерніях; Золотоніському, Переяславському і Кременчуцькому повітах Полтавської губернії; Остерському повіті Чернігівської губернії й Катеринославському повіті Катеринославської губернії [Центральний державний історичний архів України, м. Київ, ф. 442, оп. 864, спр. 279, арк. 14-15. URL: http://cdiak.archives.gov.ua/v_1914_viyna.php].

представницький орган – Українську Центральну Раду (далі – УЦР). Після Всеукраїнського національного конгресу вона з київської організації перетворилася на загальноукраїнську.

В перші місяці після створення УЦР судова система новопосталої держави за інерцією наслідувала досвід Російської імперії. Лише на початку липня 1917 р. виконавчий орган УЦР – Генеральний Секретаріат (у січні 1918 р. реформований на Раду Народних Міністрів Української Народної Республіки (далі – УНР)), визначив компетенцію Генерального Секретарства судових справ. З огляду на брак часу, вкрай необхідного для створення власного законодавства, УЦР, ухваливши 25 листопада 1917 р. Закон про правонаступництво [24, с. 9] (усі російські закони визнавалися чинними. – *Авт.*), спромоглася здійснити лише окремі кроки у сфері судочинства. Більшовицька агресія також внесла свої – негативні корективи у цей процес. Політичний провід та збройні частини молодой української держави у ніч з 8 на 9 лютого змушено залишили Київ.

Керівництво Центральної Ради, перебуваючи за межами столиці, 14 лютого 1918 р., ухвалило рішення про запровадження посад головних губернських комендантів, які мали право утворювати тимчасові військові революційні суди. Ці надзвичайні органи здійснювали кримінальне переслідування відповідно до Інструкції військовому революційному судові⁸, виданої вже після повернення УЦР до Києва – 5 березня 1918 р. [25, с. 25] Компетенція зазначених судів поширювалася на військовослужбовців і цивільних громадян у випадках вчинення ними вбивства, підпалу, згвалтування, грабежу, розбою. Цим документом встановлювалося, що провадження у військовому революційному суді могло розпочатися тільки за поданням головного губернського коменданта у разі оголошення у визначеній місцевості особливого правового режиму – воєнного стану чи облоги. Проте, згадані застереження щодо зміни підсудності, зокрема стосовно цивільних осіб, взяли до уваги винятково українські надзвичайні інституції.

Тим часом законодавчу ініціативу у сфері військового судочинства перебрала на себе іноземна союзницька мілітарна сила (німецькі та австро-угорські формування, запрошені урядом УНР для допомоги у звільненні України від більшовиків). Так, командувач німецькими військами А. Лінзінген 21 березня 1918 р. видав розпорядження про запровадження на території України законів воєнного часу, а відтак і відповідного поширення юрисдикції німецьких військово-польових судів на все без винятку населення із застосуванням смертної кари за шпигунство, державну зраду, порушення публічного спокою, заклик до повстання тощо [26, с. 54].

Свавілля німецьких та австро-угорських військових судів викликало обурення українського уряду. Народне міністерство судових справ УНР 23 березня 1918 р. видало спеціальний обіжник, у якому наголошувалося, що німецькі військові суди не мають юридичної сили, оскільки для покарання українців існують власні цивільні та військові суди [27].

Проте союзницькі сили стояли на своєму. Їх зневага до української влади та ігнорування згаданого та інших її розпоряджень виявилися у чергових демаршах. 25 квітня 1918 р. німецьке командування в особі Германа Айхгорна (Ейхгорн), який останнього березневого дня заступив на посаді свого попередника А. Лінзінгена, оголосив власні військово-польові суди виключними органами кримінальної юстиції на всій території України, де дислокувалися підпорядковані йому збройні сили. Така

⁸ Інструкція військовому революційному судові, видана 5 березня 1918 р., стала першим нормативно-правовим актом із питань судочинства, який містив нові положення, що повністю відкидали законодавчий шаблон Російської імперії.

ухвала обґрунтовувалася тим, що українські суди виявилися неспроможними підтримувати порядок. Всі громадяни, які мешкали у згаданих місцевостях, потрапляли під юрисдикцію загаданих спеціальних судів за: вчинки проти громадського порядку, кримінальні злочини проти німецьких і союзних військ, як і проти всіх осіб, що до них належать; вуличні зібрання, усну та друковану агітацію проти влади. Командування австро-угорської Східної Армії, штаб якого розміщувався в Одесі, 28 квітня 1918 р. видало аналогічне розпорядження про поширення на українських громадян юрисдикції військово-польових судів на всій території перебування своїх військ [10, с. 348].

29 квітня 1918 р. – в останній день свого існування – Українською Центральною Радою була ухвалена Конституція УНР, у якій окремий розділ присвячувався організації судової системи. Встановлювалося, що *“судова влада у рамках цивільного, кримінального і адміністративного законодавства здійснюється виключно судовими установами”*. Щоправда, у статтях розділу VIII *“Про тимчасове припинення громадянських свобод”* (ст.ст. 79 – 81) обумовлювалося, що у надзвичайних випадках держава залишає за собою право обмежувати згадані свободи [28]. Ймовірно, малося на увазі запровадження особливого правового режиму і заходів, пов’язаних з ним.

Проте основні положення Конституції УНР не були реалізовані, адже саме в цей день до влади прийшов Гетьман Павло Скоропадський, який проголосив утворення Української Держави (далі – УД). Одним з першочергових завдань гетьманської адміністрації було налагодження ефективного функціонування органів судової влади. Новий очільник держави досить негативно ставився до реформування судової системи, здійснюваної в період Центральної Ради і вважав за необхідне вдаватися до ефективних кроків. Однак, він мусив рахуватися з присутністю союзницьких військ, чий судові інституції продовжували утримувати “пальму” першості у цій сфері. Не вдаючись до різких кроків, Гетьман підійшов до цієї проблеми помірковано.

У травні 1918 р. із урядовців Міністерства судових справ (юстиції) Української Держави було утворено комісію, яка розробила пропозиції українського уряду щодо розмежування підсудності українських та німецько-австрійських судів. Пропонувалося обмежити підсудність австро-німецьких судів стосовно цивільних справ про злочини, спрямовані безпосередньо або побічно проти австро-німецьких військ. 28 травня 1918 р. на засіданні уряду міністр юстиції Михайло Чубинський доповів, що наказ Г. Айхгорна від 25 квітня 1918 р. про запровадження в Україні німецьких військово-польових судів доволі вільно трактує підлеглість українських громадян німецькій юрисдикції. Про арешти та суди над місцевими мешканцями українську сторону взагалі не повідомляли. Це ж стосувалося й австро-угорських військ. Рада Міністрів постановила ввійти щодо цих питань у зносини з німецьким та австро-угорським командуванням. Міністрам українського уряду М. Чубинському та Д. Дорошенку доручалося підготувати ноту до німецького й австро-угорського командування, вимагаючи обмеження їх юрисдикції щодо українського населення [29, с. 35].

Одночасно з підготовкою ноти, вірогідно, не маючи великих сподівань на порозуміння з адресатами офіційного звернення, пришвидшив підготовку українського закону *“Про військову підсудність”*, який з’явився 30 травня 1918 р. Документ не лише визначав протиправні діяння, що мали розглядатися військовими судами у порядку звичайної підсудності (військовослужбовці та особи, причетні до збройних сил), а й виняткової. У разі запровадження воєнного стану військовому суду підлягали цивільні особи за зраду, шпигунство, повстання проти влади, опір владі, напад на військових при виконанні ними службових обов’язків, ворожу агітацію, вбивство, розбій, грабіж, підпал, зґвалтування. Перелік злочинів практично стовідсотково співпадав з тими, які були

задекларовані у законі Російської імперії про режим воєнного стану (1892 р.), що дозволяє небезпідставно припускати пролонгацію традиції запозичень. Останнє у тих умовах було цілком зрозумілим. Але, окрім згаданого, текст закону УД містив і нові положення. Приміром, у разі ведення бойових дій на чужій території військовому суду в порядку виняткової підсудності (за відсутності там загальних судів) підлягали *“мешканці місцевостей, захоплених армією під час війни, обвинувачені у шпигунстві, повстанні проти встановленої законним шляхом влади, опорі владі, нападі на військових, ворожій агітації, знищенні військового майна”*, а також за ті види злочинів, які будуть передані до військової підсудності, згідно з окремим розпорядженням командувача армії [30].

Проте і до цього закону УД, як, зрештою, і до інших, іноземна військова влада поставилася зневажливо. Її представники не лише продовжували втручатись у діяльність українських судових установ, а й перебирали на себе ініціативу. Як і в період Центральної Ради, німецькі та австро-угорські військово-польові суди розглядали значну кількість кримінальних справ щодо цивільних осіб.

2 червня 1918 р. гетьманський уряд прийняв закон про структуру й функції Генерального Суду як вищої судової інстанції в Україні. Цей документ, окрім іншого, окреслював перспективи судової реформи.

З певним зволіканням союзники все ж розглянули пропозиції українського уряду, надіслані ще у травні 1918 р. Відповідь, підписана начальником штабу німецьких військ генералом Гренером і військовим уповноваженим австро-угорської Східної армії майором Флейшманом, надійшла 30 червня. У дописі містилася обіцянка інформувати українську владу про злочини, вчинені цивільними громадянами, і у деяких випадках допускати прокурорський нагляд. Очільники іноземних військ категорично залишили за собою розгляд справ про *“підбурювання та агітацію проти українського уряду і здійснення натовпом убивства, розбою, розгрому та інших загальних деліктів”* (правопорушень – Авт.) [31].

Дещо пізніше відбулося пом'якшення ставлення іноземної мілітарної влади до режиму виконання покарань щодо засуджених їхніми судами. 24 серпня 1918 р. цивільним особам, засудженим, зокрема австро-угорським судом, дозволили відбувати покарання *“в українській цивільній в'язниці під військовим наглядом”* [31].

Зовнішні загрози та внутрішні негаразди змусили П. Скоропадського 6 листопада 1918 р. оголосити стан *“надзвичайної охорони”* (за регламентом Російської імперії 1881 р.) у Волинській губернії. Наступного дня Гетьман запровадив такий самий правовий режим в Одесі. Воєнний стан у Миколаєві, Херсонській, Катеринославській, Подільській та північних повітах Таврійської губернії був оголошений на початку доби 9 листопада. А в ніч з 11 на 12 листопада його поширили на Чернігівську, Полтавську, Київську губернії та місто Київ [32].

Таким чином, у квітні – грудні 1918 р. військове судочинство стало домінуючим в Україні. Але військові суди Гетьманату лише формально мали широку юрисдикцію, зокрема і стосовно цивільних осіб. В реальному житті, здебільшого, вони поступалися перед засиллям іноземної – союзницької мілітаризованої Феміди, яка привласнила собі більшість повноважень у цій сфері.

Після приходу до влади Директорії УНР (14 листопада 1918 р.) розпочалася реорганізація державного апарату. Реформа торкнулася й судової системи. Республіканська влада насамперед прагнула ліквідувати здобутки гетьманського уряду і в судочинстві, зокрема, намагаючись якомога швидше відновити судові органи, утворені у період Центральної Ради.

Надзвичайно складна геополітична ситуація, в якій опинилася Україна, передусім необхідність боротьби з внутрішніми і зовнішніми противниками, головним чином з більшовиками, зумовлювали специфіку правової системи УНР, домінування у цій сфері надзвичайного судочинства.

За тиждень після виникнення Директорії – 22 листопада 1918 р. у збройних силах почали створюватися військово-польові суди, організація яких ґрунтувалася, здебільшого, на законодавстві Російської імперії (Військовому статуті про покарання 1869 р., Положенні про польове управління військ у воєнний час 1914 р.) [33, с. 115].

16 грудня 1918 р. у Києві та його приміській зоні був оголошений стан облоги. Під юрисдикцію військово-польового суду підпадали військові і цивільні особи, звинувачені в участі у будь-яких маніфестаціях і зібраннях не лише на площах і вулицях, а й у закритих приміщеннях без належного на це дозволу; у друкуванні листівок, прокламацій та відозв, порушенні комендантської години, поширенні провокаційних пліток, агітації, підбурюванні, пограбуваннях, розбійництві, вбивствах, підпалах, зґвалтуваннях, збройних нападах на військову варту і цивільних урядовців у продажу спиртних напоїв тощо [34, с. 86].

Формування надзвичайної судової системи УНР продовжувалося і в умовах запровадженого особливого правового режиму. 26 січня 1919 р., через два дні після оголошення на всій території УНР воєнного стану⁹ [35, с. 449], уряд ухвалив закон, яким ліквідовувалися військово-польові суди та прописувався порядок організації тимчасових колегіальних судових інституцій збройних сил – надзвичайних військових судів. Під юрисдикцію останніх потрапляли всі військові, а також цивільні особи за злочини, перелік яких встановлювався не лише законом, а й наказом того чи іншого військового начальника. Як для військових, так і цивільних *“кара на смерть”* (розстріл) передбачалася за: за агітацію серед військ проти УНР, шпигунство, повстання проти влади тощо. Альтернативою згаданих суворій санкції могла стати *“строчна або безстрочна каторга”*. З огляду на розміри території, яку о тій порі контролювала Директорія, згадане покарання видається глумом і над засудженими, і над самим законодавством.

Склад суду (6 осіб включно з головою та секретарем), як вже зазначалося, не був сталим. До нього у день призначеного засідання щоразу обирали нових старшин, підстаршин і навіть звичайних козаків. Видається дещо дивним застереження з тексту згаданого закону, продубльоване пізніше в змінах до нього (20 серпня 1920 р.). Декларувалося, що прокурор та секретар суду мав призначатися зі старшин *“з вищою юридичною освітою, або знайомих з судовим процесом”*. У разі відсутності таких, що було цілком зрозумілим у військах, дозволялося (! – *Авт.*) включати до складу суду *“хоча б письменних”* старшин або козаків. Вироки, винесені цими інституціями за спрощеною процедурою, не підлягали оскарженню й негайно виконувалися. Щоправда, особи, засуджені до вищої міри покарання, мали право протягом шести годин після оголошення ухвали звернутися з проханням про помилування або полегшення кари до *“Верховної влади”*, тобто Директорії, а в *“Дієвій армії до Головного отамана”* [36, с. 122].

⁹ Пропозиція про оголошення воєнного стану була внесена й схвалена на засіданні Уряду УНР ще 20 січня 1919 р. А сам Закон про запровадження згаданого особливого правового режиму та стану облоги з’явився чотирма днями пізніше – 24 січня 1919 р. У ньому, зокрема, зазначалося: *“1. Всю територію Української Народної Республіки оголосити на військовому стані. 2. Залишити Київську губернію на стані облоги...”*. У 5 та 6 пунктах йшлося про судочинство, яке мали здійснювати військові суди, організація яких регламентувалася Законом, котрий вийшов лише за два дні – 26 січня 1919 р. 5 лютого цього ж року стан облоги за поданням військового міністра був оголошений урядом УНР на території Вінницької губернії

Тимчасові військові суди, зокрема при дивізіях та корпусах Дієвої армії УНР, функціонували пів року. Через брак кваліфікованих кадрів й інші об'єктивні обставини вони були розформовані (відповідно – 14 червня і 5 липня 1919 р.). Всіма справами мав займатися суд при Генеральному штабі Дієвої армії [34, с. 88].

Система військового судочинства, що виникала стихійно, ґрунтуючись на доволі хиткій організації та правовій базі, в умовах практично необмеженої юрисдикції, часто-густо була знаряддям політичної розправи не лише з політичними опонентами, а й з палкими прихильниками незалежної України. Свідченням цьому є швидкий суд (10 червня 1919 р.) і розстріл (28 червня 1919 р.) відомого українського воєначальника Петра Болбочана. Натомість тогочасна судова система поблажливо ставилася до свавілля отаманів, поглиблюючи у такий спосіб анархію в державі [33].

На відміну від Наддніпрянщини, де судочинство Директорії орієнтувалося на Російське імперське законодавство, на території Західноукраїнської Народної Республіки (ЗУНР), з огляду на безперервні бойові дії, відповідна сфера регулювалася законами колишньої Австро-Угорської імперії. Поряд з військовими структурами створювалася й профільована юстиція. Вже 8 листопада 1918 р., під час боїв у Львові, було створено перший військово-польовий суд, під юрисдикцію якого, крім військовослужбовців української армії, підпадали цивільні особи, що вчинили *“заворушення публічного спокою, грабунок, крадіжку”* [34, с. 90]. Трохи пізніше – 21 листопада того ж року ЗУНР схвалила ряд законодавчих актів, а серед них і декрет про *“Тимчасову організацію судівництва”* [37, с. 154].

Розпорядженням Державного Секретаріату ЗУНР від 3 грудня 1918 р. при кожному окружному військовому підрозділі (команді) було створено військово-польові суди, під юрисдикцію яких підпадали і цивільні особи. Перелік злочинів, за вчинення яких останні потрапляли до поля зору військової Феміди ЗУНР, був уточнений розпорядженням Державного Секретаріату від 17 лютого 1919 р. Йшлося, зокрема, про зраду батьківщини, повстання проти легітимної влади, знищення телеграфних і телефонних ліній та військового майна. У зв'язку з тим, що дані положення по-різному інтерпретувалися судами, Державний секретаріат 1 березня 1919 р. видав спеціальне роз'яснення: цивільні особи підпадали під юрисдикцію військових судів лише у разі шкідництва та ведення більшовицької агітації і пропаганди [34, с. 93].

Після переходу Української Галицької Армії за р. Збруч було дещо змінено структуру військово-судових органів. На жаль, історичні джерела не зберегли майже ніякої інформації щодо їх діяльності у досліджуваній проблематиці.

Висновки.

Узагальнюючи викладене, слід підкреслити, що на українських землях паралельно з появою регулярного війська в умовах збройних конфліктів (або й за відсутності таких) поступово формувалася система надзвичайного судочинства, яка охоплювала не лише військових, а й пересічних громадян.

Розвиток відповідних інституцій, їх повноваження залежали від світоглядних і політичних уподобань влади, або особи, що її уособлювала. Рівень суворості покарання, як і перелік злочинів, були позначені специфічними рисами кожного з історичних періодів та чинного права. Законодавчо закріплені норми щодо покарання цивільних осіб регламентувалися спочатку у межах звичаєвого права, згодом – наприкінці XVIII ст. – упродовж першої половини XIX ст. в окремих законодавчих розрізнених актах часто-густо із запозиченням досвіду іноземних держав, зокрема Франції.

Вже в останні десятиліття XIX ст. викристалізувалася система регламентних документів, які фіксували межі кримінальної та адміністративної відповідальності

цивільних осіб у межах запроваджуваних особливих правових режимів. Наприкінці XIX ст. – на початку XX ст., зокрема напередодні Першої світової війни, вони перетворилися на постійно діючі адміністративні режими управління державою та суспільством. Місце судів заступила адміністративна та військова (швидка/закрита) розправа. Таким чином створювалася атмосфера пролонгованого свавілля.

У період національно-визвольних змагань 1917 – 1921 рр. кожна зміна уряду в Україні супроводжувалася використанням надзвичайного/воєнного стану, зумовленого ворожим оточенням, перманентними бойовими діями і внутрішньою нестабільною політичною ситуацією. За доби Центральної Ради в умовах війни, розв'язаної більшовицькою Росією, на розбудову дієвого державного апарату, збройних сил і спецслужб не вистачало часу. Бракувало досвіду, а часто-густо й політичної волі для запровадження всіх вкрай необхідних реформ. Судова система мала змішаний та, до певної міри, хаотичний характер.

Українська Держава гетьмана Павла Скоропадського в умовах конфлікту з більшовицькою Росією та гострого протистояння з політичними опонентами змушено пішла на компроміс з представниками іноземних армій, запрошених попередньою верхівкою УНР. З огляду на ці та інші об'єктивні обставини, домінувало надзвичайне судочинство, а цивільні особи опинилися у полі зору військової Феміди.

Спільними рисами всіх форм державності на українських землях була рецепція права попередньої влади чи то Російської імперії, чи то Австро-Угорщини. Хоча запозичення цих норм відбувалося у відповідності до специфічних умов суспільно-політичного розвитку країни та зовнішньополітичних чинників, які через перманентний воєнний стан формували особливі умови розвитку судочинства, скеровуючи його в рамки жорстких норм. Порівняно із надзвичайним законодавством інших держав, яке передбачало і регламентувало або воєнну, або цивільну диктатуру, на українських землях, які входили до складу Російської імперії особливий правовий режим одночасно мав ознаки обох диктатур.

У часи національно-визвольних змагань 1917 – 1921 рр. жоден з українських урядів так і не спромігся ухвалити власні закони про особливі правові режими, зокрема й судочинство в умовах воєнного стану. Як слушно зауважив український історик Віталій Скальський: *“Суспільство пережило чотири роки війни, кілька переворотів, прихід та відступ більшовиків з їх червоним терором... А [українська] влада не зловживала своїми надзвичайними повноваженнями. Може, й дарма. Бо Україна стрімко наближалась до чергових політичних потрясінь”* [32].

Використана література

1. Гессен В.М. Исключительное положение. Санкт-Петербург, 1908. 411 с.; Гессен В.М. “Исключительное положение”. Харків: Еспада, 2005. 240 с. URL: <http://ex-jure.ru/law/news.php?new sid=367>
2. Александров О.Г. Чрезвычайное законодательство в России во второй половине XIX – начале XX в.: дис. канд. юрид. наук. Нижний Новгород, 2000. 161 с.; Зиборов О.В. Институт военного положения по российскому праву (историко-правовое исследование): дис. ...канд. юрид. наук. Москва, 2002. 222 с.; Обухов В.В. Правовые основы организации и деятельности военных трибуналов войск НКВД СССР в годы Великой Отечественной войны 1941 – 1945 гг. (историко-правовое исследование): дис. ...кандидата юрид. наук: 12.00.01. Москва, 2002. 228 с.; Пчелинцев С.В. Проблемы ограничения прав и свобод граждан в условиях особых правовых режимов: монографія. Москва: Норма, 2006. 480 с.; Никонов Д.А. Советское чрезвычайное военное законодательство (1920–1941 гг.): монография; под ред. Белозерова Б.П. С-Пб.: С-Пб ВИ ВВ МВД России, 2006. 206 с.

3. Вовк Ю.С. Судові органи Української народної Республіки та Української держави (1917 – 1920 рр.): автореф. дис. ...канд. юрид. наук: 12.00.01. Львів: Нац. ун-т ім. І. Франка. 2000. 19 с.; Рум'янцев В. Судова система в Україні за часів Директорії. *Вісник Академії правових наук України*. 2001. № 4(27). С. 84-94; Тимошук О.В. Охоронний апарат Української Держави (квітень – грудень 1918 р.): монографія. Харків: Вид-во Ун-ту внутр. справ, 2000. 462 с.; Історія держави і права України. Академічний курс: у 2-х т. / під ред. В.Я. Тація, А.Й. Рогожина. Київ, 2000. 396 с.; Ярмиш О.Н. Каральний апарат самодержавства в Україні в кінці XIX – на початку XX ст. Харків, 2001. 288 с.
4. Судова влада в Україні: історичні витоки, закономірності, особливості розвитку / авт. кол.: В.С. Бігун, І.Й. Бойко, Т.І. Бондарук, К.А. Віслобоков, О.А. Гавриленко, Л.О. Зайцев, А.Ю. Іванова, О.О. Малишев, І.В. Музика, В.Т. Окіпнюк, Є.В. Ромінський, О.О. Самойленко, М.І. Сірий, І.Б. Усенко (кер. кол.), М.Д. Ходаківський, Л.В. Худояр, О.Н. Ярмиш. – (НАН України. Інститут держави і права ім. В.М. Корецького; Міжнародна асоціація істориків права). Київ: “Наукова думка”, 2014. 503 с.
5. Тисяча років української суспільно-політичної думки. У 9-ти т. Т. 1: (X – XV ст.) / упоряд. О. Сліпушко; ред. тому Ю. Косенко. Київ: Дніпро, 2001. 632 с.
6. Атаманова Н.В. Литовські статuti як історичні пам'ятки у системі вітчизняних джерел права. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція*. 2014. Т. 1. С. 22-24.
7. Статут Вялікага княства Літоўскага 1566 г. Мінск, 2003. С. 35-263; Філінюк І.Г. Військове судочинство доби Великого князівства Литовського. *Актуальні проблеми держави і права*. Одеса, 2009. Вип.49. С. 132-138.
8. Щербак В.О. Українське козацтво: формування соціального стану. Друга половина XV – середина XVII ст. Київ, 2000. URL: <http://litopys.org.ua/coss1/shch03.htm>
9. Бедрій М.М. Козацьке право як історичний тип українського звичаєвого права (XVI ст. – 40 рр. XIX ст.). *Вісник Львівського університету. Сер. юридична*. 2015. Вип. 61. С. 78-86; Суди і покарання у козаків Запорізької Січі: URL: https://protocol.ua/ua/sudi_i_pokarannya_u_kozakiv; Гамбург Л.С. Козацькі суди та порядок розгляду справ у судово-адміністративних органах Гетьманщини. *Енциклопедія історії України*. Т. 4: Ка-Ком / редкол.: В.А. Смолій (голова) та ін. НАН України. – (Інститут історії України). Київ: “Наукова думка”, 2007. 528 с.
10. Судова влада в Україні: історичні витоки, закономірності, особливості розвитку / відп. ред. І.Б. Усенко. Київ: “Наукова думка”, 2014. 501 с.
11. Рекотов П.В. Австро-угорське кримінальне законодавство на західноукраїнських землях (друга половина XVIII – XIX ст.). URL: http://www.zgia.zp.ua/gazeta/MNPKMF17_112.pdf
12. Формирование особой военно-судебной системы в ходе реформ Петра I: URL: <https://lawbook.online/gosudarstva-prava/formirovanie-osoboy-voenno-sudebnoy-sistemyi-39024.html>; Загорский Г. Становление военно-судебных органов в эпоху правления Петра I: URL: <https://elibrary.ru/item.asp?id=28083846>
13. Вронська Т.В., Лисенко О.Є., Шандра О.І. Режими воєнного та надзвичайного стану на українських землях у другій половині XIX – на початку XX ст. *Український історичний журнал*. 2017. № 5. С. 40-54.
14. Полное собрание законов Российской империи. Т. 39. Санкт-Петербург, 1867. Отд. 2: 1864. № 414476. Ст. 226.
15. Полное собрание законов Российской империи. Собр. 2-е. Т. 52. Санкт-Петербург, 1879. Отд. 1: 1879. № 57156.
16. Пчелинцев С.В. Суды в условиях особых правовых режимов. *Отечественные записки*. 2000. № 2. URL: <http://www.strana-oz.ru/2003/2/sudy-v-usloviyah-osobyyh-pravovyh-rezhimov>
17. Полное собрание законов Российской Империи. Собр. 2-е. Т. 54. Санкт-Петербург, 1881. Ст. 59491.
18. Полное собрание законов Российской империи. Собр. 3-е. Т. I. Со дня возшествия на престол Государя Императора Александра Александровича 31 декабря 1881 года. Отд № 1-585 и Дополнения. Санкт-Петербург, 1885. С. 261-266.

19. Полное собрание законов Российской Империи. Собр. 3-е. Т. 1. Санкт-Петербург, 1885. Отд.1. 1881. № 382.
20. Полное собрание законов Российской Империи. Собр. 3-е. Т. 12. Санкт-Петербург, 1895. № 8757.
21. Пчелинцев С.В., Исхакова О.А. Военно-полевые суды. URL: http://www.stolypin.ru/proekty-fonda/entsiklopediya-petr-arkadevich-stolypin/?ELEMENT_ID=327
22. Долженко А.Н. Військово-польовий суд. Юридична енциклопедія / ред. Ю.С. Шемшученко та ін. – (НАН України, Ін-т держави і права ім. В. М. Корецького). Київ: “Українська енциклопедія”, 1998 – 2004. Т. 1: А–Г. 1998. 669 с. URL: https://leksika.com.ua/10120321/legal/viyskovo-poloviy_sud
23. Кирієнко О.Ю. Діяльність органів військової цензури 1914 – 1917 рр. *Український історичний збірник*. 2009. Вип. 12. С. 160.
24. Вовк Ю.Є. Створення Центральною Радою судової системи в Україні (1917 – 1918 рр.): зб. навч.-метод. матеріалів і наук. ст. іст. ф-ту. Волин. держ. ун-ту. ім. Лесі Українки. Луцьк, 1999. Вип. 4. С. 9-15.
25. Середа А.М. Інституалізація судової влади в добу відродження української державності 1917 – 1918 рр.). *Вісник Запорізького національного університету* 2017. № 3. С. 20-31.
26. Пиріг Р.Я. Центральна Рада й німецьке військове командування в Україні: проблеми взаємовідносин (лютий – квітень 1918 р.). *Український історичний журнал*. 2007. № 2. С. 47-63.
27. Гуцалюк О.І. Суд і судочинство на Волині в період правління Української Центральної ради (березень 1917-го – квітень 1918 року) URL: file://Tamara/Downloads/Nvvnui_2014_7_10.pdf
28. Конституція Української Народньої Республіки (Статут про державний устрій, права і вільності УНР). Державні утворення (1917 – 1920); Історичний документ, Конституція від 29.04.1918. *База даних Законодавство України ВР України*. URL: <https://zakon.rada.gov.ua/laws/show/n0002300-18>
29. Фельдмаршал Герман Айхгорн: служба та смерть в Україні (квітень – липень 1918 р.). *Український історичний журнал*. 2017. № 3. С. 24-45.
30. Сидоренко А.С. Військова політика Української держава Гетьмана П. Скоропадського. *Вісник КНЛУ. Сер. Історія, економіка, філософія*. 2015. Вип. 20. С. 140-153.
31. Тимошук О.В. Охоронний апарат Української Держави (квітень – грудень 1918 р.): історико-правове дослідження: автореф. дис. ...д-ра. юрид. наук: 12.00.01. Одеса: Нац. ун.-т “Одеська юридична академія”. 2000. 40 с.
32. Скальський В.В. Як Гетьман військовий стан запроваджував. *Історична правда*. 26 листопада 2018 р. URL: <https://www.istpravda.com.ua/columns/2018/11/26/153324>
33. Сідак В.С., Осташко Т.С., Вронська Т.В. Полковник Петро Болбочан: трагедія українського державника: наукове видання. Київ: Темпора, 2004. 416 с.
34. Рум’янцев В.О. Судова система в Україні за часів Директорії. *Вісник Академії правових наук України*. Харків: Право, 2001. № 4(27). С. 84-94.
35. Директорія, Рада Народних Міністрів Української Народної Республіки. Листопад 1918 – листопад 1920 рр.: документи і матеріали. У 2-х т., 3-х ч. Т. 2. – (НАН України. Ін-т історії України; ЦДАВО України; Дослідний ін-т сучасної укр. історії (Філадельфія); упоряд.: В. Верстюк (кер.) та ін. Київ: Вид-во ім. Олени Теліги, 2006. Т. 2. 744 с.
36. Закон про надзвичайні військові суди: Закон УНР від 26.01.19 р. *Вістник Державних Законів Української Народної Республіки*. 1919. 18 лютого. Вип. 8. Ч. 102. С. 58-60.
37. Копиленко О.Л., Копиленко М.Л. Держава і право України: 1917 – 1920 рр.: підручник. Київ: Либідь, 1997. 208 с.

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

## До відома авторів

“ІНФОРМАЦІЯ І ПРАВО” – спеціалізований науковий фаховий журнал по результатах фундаментальних і прикладних наукових досліджень, а також дисертаційних робіт на здобуття наукових ступенів кандидата наук (доктора філософії) та доктора наук з проблем права та інформаційного законодавства, правової інформатики, інформаційних технологій, інформатизації, інформаційної і національної безпеки та інформаційних ресурсів в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має описувати та науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямками досліджень, як:

**інформаційне право; правова інформатика, інформаційна і національна безпека.**

## Вимоги до оформлення

1) Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:

- у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;
- параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;
- відстань між рядками – 1 інтервал;
- кількість матеріалу однієї статті – не більше 15 стор.

Стаття має передбачати такі обов’язкові структурні елементи:

- УДК.
- Ім’я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи, а також – ідентифікатор ORCID, при наявності.
- Назва статті (укр. та англ. мовами).
- Анотація та ключові слова (укр., англ. та рос. мовами).
- **Розв’язання проблеми**, шляхом наукового вирішення завдання:
  - **постановка проблеми** (загальна характеристика);
  - **результати аналізу наукових публікацій** – надаються відомості про стан вирішення проблеми та ПІБ авторів, з обов’язковим посиланням на їхні роботи (в [...]), повний опис бібліографії яких вказується в підрозділі “Використана література”; виділяються не вирішені раніше частини проблеми, які будуть вирішуватися в статті; наводяться аргументи, що підтверджують актуальність і новизну роботи;
  - **формування мети** (постановка завдання) статті;
  - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
- **Висновки** за результатами розв’язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
- **Використана література.** Бібліографічний опис списку використаної літератури може оформлятися автором за його вибором з урахуванням Національного стандарту України ДСТУ 8302:2015 “Інформація та документація. Бібліографічне посилання. Загальні положення та правила складання” або зі стилем OSCOLA (Стандарт Оксфордського університету для цитування юридичних документів), які віднесені п. 11. Наказу МОН України від 12.01.17 р. № 40 до рекомендованого переліку стилів оформлення списку наукових публікацій.
- Підпис, адреса (е-адреса), телефон автора.

**2) Подавати письмовий Відгук на статтю, підписаний особою, яка має науковий ступінь.**

Відгук має бути чітко структурований та обґрунтований згідно з такими частинами:

- *Актуальність теми.*
- *Новизна та обґрунтованість одержаних результатів.*
- *Наукова (практична) цінність результатів.*
- *Висновок про можливість відкритої публікації.*

**3) Рукопис статті та Відгук мають бути ретельно вчитаними, виправленими і підписаними відповідними особами.****4) Окремим файлом автори подають електронну версію розширеної анотації статті (до 1 сторінки формату А-4) англійською мовою, яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України “Про затвердження порядку формування переліку наукових фахових видань України” від 17.10.12 р. № 1111.****5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, пропонується здійснити оплату в розмірі 420 грн. на рахунок Інституту.**

**Реквізити для оплати робіт:**

*Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р UA288201720313201002201011870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).*

**Адреса редакції:** 01032, м. Київ, вул. Саксаганського, 110-В.

**6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net**

### **Д о у в а г и**

- Вчена рада НДПП НАПрН України не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції. Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за 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

**№ 2(33)/2020**

|                                               |                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Засновники журналу:                           | <ul style="list-style-type: none"> <li>- Науково-дослідний інститут інформатики і права Національної академії правових наук України (НДІП НАПрН України);</li> <li>- Національна бібліотека України ім. В.І. Вернадського Національної академії наук України;</li> <li>- Відкритий міжнародний університет розвитку людини “Україна”.</li> </ul>                 |
| Видавець:                                     | © НДІП НАПрН України.                                                                                                                                                                                                                                                                                                                                            |
| Адреса редакції:                              | 01032, м. Київ, вул. Саксаганського, 110-В.<br>Науково-дослідний інститут інформатики і права<br>Національної академії правових наук України.<br>Тел.: 234-94-56; e-mail: bvm777@ ukr.net                                                                                                                                                                        |
| Веб-сторінки журналу у мережі Інтернет:       | URL: //www.ippi.org.ua – НДІП НАПрН України;<br>URL: //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.                                                                                                                                                                                                                                          |
| Founders of journal:                          | <ul style="list-style-type: none"> <li>- Scientific Research Institute of Informatics and Law of the National Academy of Law Sciences of Ukraine (SRIIL of the NALS of Ukraine);</li> <li>- Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine;</li> <li>- Open International University of Human Development “Ukraine”</li> </ul> |
| Publisher:                                    | © SRIIL of the NALS of Ukraine.                                                                                                                                                                                                                                                                                                                                  |
| Address of release:                           | 01032, Kyiv, Saksaganskogo str., 110-V.<br>Scientific Rresearch Institute of Informatics and Law<br>of the National Academy of Law Sciences of Ukraine.<br>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;<br>URL: //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National Academy of Sciences of Ukraine.                                                                                                                  |