

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

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(28)/2019

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

Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12),
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів кандидата наук (доктора філософії – Ph.D.)
і доктора наук у галузі юридичних наук.

Друковане періодичне видання ІНФОРМАЦІЯ І ПРАВО внесене в міжнародну базу даних
періодичних видань, згідно відповідного номеру ISSN.

м. Київ

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

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

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND LAW

SCIENTIFIC PROFESSIONAL JOURNAL

№ 1(28)/2019

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

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

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

УДК 002:340+316.4+338.46

Р е д а к ц і й н а к о л е г і я

ПИЛИПЧУК Володимир Григорович, доктор юридичних наук, професор, член-кореспондент
НАПрН України – *голова редакційної колегії,
головний редактор;*

БРИЖКО Валерій Михайлович, доктор філософії (Ph.D.) з юридичних наук, с.н.с.
– *зас. голови редакційної колегії,
зас. головного редактора;*

ПОПИК Володимир Іванович, доктор історичних наук, професор,
член-кореспондент НАН України – *зас. голови редакційної колегії;*

БЕБИК Валерій Михайлович, доктор політичних наук, професор – *зас. голови редакційної колегії;*

АРИСТОВА Ірина Василівна, доктор юридичних наук, професор;

БАРАНОВ Олександр Андрійович, доктор юридичних наук, с.н.с.;

БЄЛЯКОВ Костянтин Іванович, доктор юридичних наук, професор;

ДЗЬОБАНЬ Олександр Петрович, доктор філософських наук, професор;

ДОВГАНЬ Олександр Дмитрович, доктор юридичних наук, с.н.с.;

КОПАН Олексій Володимирович, доктор юридичних наук, професор;

КОРЖ Ігор Федорович, доктор юридичних наук, с.н.с.;

КУЙБИДА Василь Степанович, доктор наук з державного управління, професор;

ЛАНДЕ Дмитро Володимирович, доктор технічних наук, с.н.с.,

МАРУЩАК Анатолій Іванович, доктор юридичних наук, професор;

НАСТЮК Василь Якович, доктор юридичних наук, професор,
член-кореспондент НАПрН України;

НОР Василь Тимофійович, доктор юридичних наук, професор,
академік НАПрН України;

ОНИЩЕНКО 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.

* * * * *

UDC 002:340+316.4+338.46

E d i t o r i a l B o a r d

PYLYPCHUK Volodymyr, Doctor of Juridical Science, Professor,
Corresponding Member NALS of Ukraine – *Chairman of Editorial Board,*
– *Editor in Chief;*

BRYZHKO Valerii, Doctor of Philosophy (Ph.D.) of Juridical Science, Senior researcher fellow
– *Vice-chairman of Editorial Board,*
– *Vice-Editor;*

POPYK Volodymyr, Doctor of Historical Sciences, Corresponding Member NAN of Ukraine
– *Vice-chairman of Editorial Board.*

BEBYK Valerii, Doctor of Political Sciences, Professor – *Vice-chairman of Editorial Board;*

ARISTOVA Iryna, Doctor of Juridical Science, Professor;

BARANOV Oleksandr, Doctor of Juridical Science, Senior researcher fellow;

BIELIAKOV Konstantyn, Doctor of Juridical Science, Professor;

DZOBAN Oleksandr, Doctor of Philosophical Science, Professor;

DOVGAN Oleksandr, Doctor of Juridical Science, Senior researcher fellow;

KOPAN Oleksii, Doctor of Juridical Science, Professor;

KORZH Ihor, Doctor of Juridical Science, Senior researcher fellow;

KUIBIDA Vasyl, Doctor of Administration Science, Professor;

LANDE Dmytro, Doctor of Engineering Sciences, Senior researcher fellow;

MARUSHCHAK Anatolii, Doctor of Juridical Science, Professor;

NASTIUK Vasyl, Doctor of Juridical Science, Professor,
Corresponding Member NALS of Ukraine;

NOR Vasyl, Doctor of Juridical Science, Professor,
Academician NALS of Ukraine;

ONISHCHENKO Oleksii, Doctor of Philosophical Science, Professor;
Academician NALS 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;

TYKHYI 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.

* * * * *

З М І С Т

Інформаційне право

ДЗЬОБАНЬ О.П., РУБАН О.О. Сучасна людина: безпекові проблеми адаптації до нового інформаційного середовища.....	9
КОРЖ І.Ф. Право на відкриті дані – як право приватного характеру.....	19
ДОРОНІН І.М. Цифровий розвиток та національна безпека у контексті правових проблем.....	29
ТИХОМИРОВ О.О. Інформаційний делікт як підстава “інформаційної” юридичної відповідальності: відмітні ознаки.....	37
КУШНІР І.П. Адміністративна відповідальність за порушення законодавства про інформацію у прикордонній сфері.....	45
КРАВЧУК І.М. Правові особливості інформаційних суспільних відносин при наданні дистанційних адміністративних послуг.....	52
БЕЖЕВЕЦЬ А.М. Правовий статус роботів: проблеми та перспективи визначення....	61

Правова інформатика

БРАЙЧЕВСЬКИЙ С.М. Резонансні явища в системах Інтернету речей.....	68
ЛАНДЕ Д.В., ДМИТРЕНКО О.О., РАДЗІЄВСЬКА О.Г. Побудова онтологій в галузі права за даними сервісу Google Scholar.....	74

Інформаційна і національна безпека

ДОВГАНЬ О.Д., ТКАЧУК Т.Ю. Концептуальні засади законодавчого забезпечення інформаційної безпеки України...	86
ГРЕБЕНЮК М.В., ЛЕОНОВ Б.Д. Актуальні проблеми забезпечення інформаційної безпеки електоральних процесів: аналіз зарубіжного досвіду.....	100
ГАВЛОВСЬКИЙ В.Д. Аналіз стану кіберзлочинності в Україні.....	108
ГУЦАЛЮК М.В. Сучасні тенденції організованої кіберзлочинності.....	118
ТКАЧУК Н.А. Стан та проблемні питання реалізації Стратегії кібербезпеки України.....	129

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

ТУБОЛЬЦЕВА Я.С. Виключні особливості розвитку інституту усиновлення у вітчизняному цивільному процесуальному праві.....	135
ГОЛОВКО О.М. Право на інформацію щодо альтернативних методів вирішення спорів.....	144

До відома авторів152

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. 13.5. Тираж 100 прим.

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

04050, м. Київ, вул. Мельникова, буд. 63.

Свідоцтво про внесення суб’єкта видавничої справи до державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: Серія № ДК № 4779 від 15.10.14 р.

Рекомендовано до друку Вченою радою НДІП НАПрН України, протокол № 2 від 27.03.19 р.

TABLE OF CONTENTS

Informative Law

DZOBAN O., RUBAN O. Modern person: security problems of adaptation to the new information environment.....	9
KORZH I. Right to open data – as a private right.....	19
DORONIN I. Digital development and national security in the context of legal issues.....	29
TYKHOMYROV O. Information delict as an “information” legal responsibility basis: specific features.....	37
KUSHNIR I. Administrative responsibility for violation of legislation on information in border sphere.....	45
KRAVCHUK I. Legal peculiarities of information public relations in the process of providing distant administrative services.....	52
BEZHEVETS A. The legal status of robots: problems and perspectives of determination.....	61

Legal Informatics

BRAYCHEVSKYY S. Resonant phenomena in the systems of the Internet of Things.....	68
LANDE D., DMITRENKO O., RADZIEVSKA O. Construction of ontologies in the field of law according to the service Google Scholar.....	74

Informative and National Safety

DOVGAN O., TKACHUK T. Conceptual principles of legislative providing of informative security of Ukraine.....	86
HREBENIUK M., LEONOV B. Actual problems of ensuring information security in electoral processes: an analysis of a foreign experience.....	100
GAVLOVSKI V. Analysis of the state of cybercrime in Ukraine.....	108
GUZALUK M. Modern trends in organized cybercrime.....	118
TKACHUK N. Current state and problematic in the implementation of the cybersecurity strategy of Ukraine.....	129

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

TUBOLCEVA Y. Exclusive features of development of institute of adoption in the domestic civil processal law.....	135
GOLOVKO O. The right to information about alternative dispute resolution methods	144

For the consideration of authors	152
---	------------

Recommended for publication by the SRIIL of the NALS of Ukraine, protocol № 2 dated 27.03.19
--

Інформаційне право

УДК 316 (477)

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

СУЧАСНА ЛЮДИНА: БЕЗПЕКОВІ ПРОБЛЕМИ АДАПТАЦІЇ ДО НОВОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА

Анотація. У статті акцентується увага на основних соціальних проблемах безпечної адаптації людини до мінливих умов інформаційного суспільства, якими пропонується вважати: проблему мовної комунікації, що становить ядро інформатизації, та проблему інформаційної безпеки особистості. Обґрунтовується, що інформаційні технології, ставши стрижнем сучасної цивілізації, змінюють не просто якість і зміст життя сучасної людини, вони загрожують трансформувати сам спосіб її буття у світі, тому перехід до інформаційного суспільства може мати непередбачувані наслідки.

Ключові слова: інформаційне суспільство, комунікація, інформаційні технології, людина, мережеві комунікації.

Summary. The article focuses on the major social problems of safe human adaptation to changing conditions of the information society. The following issues are proposed for consideration in this regard: the problem of language communication as a core of informatization, and the problem of personal information security. It is proved that information technology, becoming a modern civilization core, change not only quality and content of modern life, they threaten to transform the very way of human existence in the world, so the transition to the information society can have unpredictable consequences.

Keywords: information society, communication, information technology, people, communication network.

Аннотация. В статье акцентируется внимание на основных социальных проблемах безопасной адаптации человека к меняющимся условиям информационного общества, которыми предлагается считать: проблему языковой коммуникации, составляющей ядро информатизации, и проблему информационной безопасности личности. Обосновывается, что информационные технологии, став стержнем современной цивилизации, меняют не просто качество и содержание жизни современного человека, они угрожают трансформировать сам способ его бытия в мире, поэтому переход к информационному обществу может иметь непредсказуемые последствия.

Ключевые слова: информационное общество, коммуникация, информационные технологии, человек, сетевые коммуникации.

Постановка проблеми. Інформаційне суспільство як суспільство нового типу, має низку особливостей у порівнянні з попередніми типами суспільств. Відбувається різке збільшення кількості інформаційних потоків і технічних засобів, що не тільки забезпечує циркуляцію інформації в суспільстві, але й забезпечує життєздатність інформаційного суспільства, виявляє нові проблеми і труднощі у соціальній комунікації і соціальній взаємодії в цілому. У різних сферах людської діяльності спостерігаються процеси інтеграції, що спричиняють процес глобалізації. З'являється єдина глобальна

комунікаційна система, що забезпечує людство великими обсягами досяжної інформації. Як наслідок, виникають нові форми комунікації, викликані розвитком глобальної комунікаційної системи. Важливою умовою для функціонування особистості у сучасному інформаційному середовищі стають процеси соціальної комунікації, які стали можливими завдяки віртуалізації сучасного суспільства. Зміни у сфері виробництва, у культурному середовищі, у мовному середовищі спричиняють зміну в моделях поведінки людини.

Відповідно, у процесі динаміки інформаційного суспільства змінюються й соціальні відносини, де стають характерними тенденції до концентрації, бюрократизації й монополізації у сфері масово-інформаційних процесів. Це примушує по-новому поглянути на певні зміни у структурі соціальної системи. Перенесення процесів фізичної соціальної взаємодії у середовище симуляцій актуалізує коригування погляду на проблему інтеграції людини.

Результати аналізу наукових публікацій свідчать, що проблеми інформаційного суспільства й існування людини в ньому є достатньо популярними у новітньому науковому дискурсі, як у закордонному (Т. Аревало, В. Бурес, М. Кокелберг, Г. Рамос, Д. Рубен, Г. Шандл та ін.) [1 – 4], так і у вітчизняному (Н. Богданович, В. Воронкова, О. Дроздовська, О. Кивлюк, А. Михальчук, Т. Тюріна та ін.) [5 – 9].

Разом з тим, вивчення даної проблеми дозволяє констатувати, що незважаючи на досить широку наявну теоретичну базу досліджуваних феноменів, потребують деяких уточнень з урахуванням нових інформаційно-технологічних процесів саме проблеми інтеграції людини в інформаційний континуум сучасного інформаційного середовища.

Метою статті є спроба осмислення основних особливостей адаптації людини до умов інформаційного суспільства.

Виклад основного матеріалу. Соціум сьогодні – це комунікаційна система, де постійно здійснюється обмін інформацією та думками, і де кожен член суспільства має право на доступ до інформації, на відстоювання власної позиції. Людина є однією з ланок, що об'єднує всю суспільну систему. Вона водночас виступає як суб'єктом, так і об'єктом діяльності, соціальних інтересів, потреб та духовно-моральних цінностей, ідеалів, переконань і прагнень. Безпосередньо пов'язані з інформаційною сферою моральні цінності істотно впливають на поведінку й діяльність людини, формують всю систему її індивідуально-суспільних відносин. Саме людина як найвища соціальна цінність акумулює в основних формах своєї життєдіяльності й інформаційне фіксує взаємозв'язок матеріального й духовного, відображаючи в цілісному вигляді життя як об'єктивну реальність, де виявляються внутрішньо взаємозалежні її інтереси, моральні цінності, ідеали, її культура, релігійні вподобання та суб'єктивне розуміння сенсу життя. Суспільство стає тією універсальною матеріально-духовною сферою, в якій особистість реалізує себе цілісно. З іншого боку, разом із соціально-економічними та політичними трансформаціями інформаційного суспільства відбувається процес переоцінки духовних цінностей, формування принципово нових засад моралі. Усе це ускладнює процес формування особистості в нинішніх інформаційних умовах.

Одним з найважливіших і найвідповідальніших з безпекової точки зору аспектів адаптації соціальної системи до нових форм життєдіяльності в інформаційному суспільстві та формування у ньому соціокультурних принципів взаємозв'язку між державою і суспільством є розвиток ринку інформаційних послуг. Він формується, з одного боку, завдяки виникненню і розвитку потреб держави, корпоративних структур, окремих індивідів й установ, тобто клієнтів, в нових типах і видах інформаційних послуг, а з іншого – внаслідок розвитку специфічних видів інформаційної комерційної діяльності, що мають самостійне соціальне значення (реклама, маркетинг, тощо). Тож сукупна

соціальна діяльність інформаційного суспільства розвивається за рахунок виявлення соціально й культурно значущих напрямків інформаційної діяльності та розширення сфер її застосування. Це значною мірою трансформує характер, форми і типи соціокультурних взаємодій. Цей аспект розвитку системи діяльностей видається одним з найактуальніших для розвитку інформаційного суспільства, в якому соціальний статус, рівень освіти й статків залежать від якості і надійності інформаційно-комунікативних взаємодій, в які включена людина як суб'єкт і як об'єкт інформаційної діяльності. Розповсюдження інформаційних технологій як у сфері виробництва, так і в гуманітарній сфері, викликало цілу низку спеціально орієнтованих послуг з обробки й використання інформації та засобів комунікації, що визначають форми перетворення соціального середовища з метою створення умов для функціонування інформаційного суспільства.

Поширення інформаційних технологій супроводжується віртуалізацією всіх сфер людського життя, перетворившись з простої технології на інформаційно-комунікативне середовище. На сьогоднішній день розширення її впливу відбувається у двох основних взаємопов'язаних напрямках: збільшення впливу віртуальності на світ реальний і віртуалізація самої реальності, які проявляються у надбанні віртуального статусу усіма сферами світу людини й соціокультурної реальності. Технічні засоби й інформаційні прийоми організації віртуальної реальності здатні кардинально змінити характер і зміст життєдіяльності як людини, так і соціуму в цілому. А отже, усвідомлення й оцінка соціальних меж, а також соціокультурних пріоритетів інформатизації дозволяє актуалізувати саме ті аспекти технологій, які спрямовані на розвиток людської життєдіяльності в різних галузях виробництва, науки, мистецтва, освіти, торгівлі, сфери обслуговування.

Масштабність проникнення віртуальної реальності в соціальне життя дає підставу вести мову про "віртуалізацію" суспільства, яка змінює спосіб життя людей, роблячи його синтетичним, посилюючи прагнення потрапити в нові її шари. Віртуальність є тотальною й безмежною, вона охоплює дедалі більшу кількість сфер суспільного життя: "віртуальний світ", "віртуальна економіка", "віртуальна політика", "віртуальна любов", "віртуальний театр". Очевидним стає постійне прискорення віртуалізації суспільства й людини, викликане збільшенням "картин світу" і віртуалізацією дійсності. Це дає право вести мову про безперервне збільшення реальностей, поліархія яких стала головним девізом сучасності. У віртуальній реальності поступово зникають просторові та часові розмежування, стираються міждержавні кордони, пропагуються нові цінності, моделі поведінки, світоглядні стереотипи. Феномен віртуалізації життєвого простору людини та суспільства характеризує принципово новий тип символічного існування людини, соціуму, культури [10, с. 110-111].

Інформаційне суспільство визначається через параметр нової особистості: простір мультиплікації можливостей людини, що несе нові виклики особистісної ідентичності, при яких зовнішні (технологічні) розширення людини перестають нею сприйматися як штучні. Інтервенція нових способів символізації, віртуалізація соціальних просторів, децентрація соціальних зв'язків посилюють динаміку і трансформують характер спілкування. Симбіоз людини з технологіями став розглядатися як такий, що здатний докорінно покращити людину, перетворивши її в якийсь новий вид. Деякі автори, що свідомо подолали технократизм, також з безпекової точки зору прогнозували соціальні, соціокультурні та особистісні наслідки техніко-технологічних змін інформаційного суспільства: трансформація біологічних фаз життєдіяльності людини, неминучість адаптації індивіда до логіки і коду електронної системи і ін. Інформаційне суспільство є епохою інформаційного

індивіда в умовах перемоги електронної (аудіовізуальної) комунікації, багаторазово підсилює інтелектуальні здібності та творчі можливості особистості [11].

Серед характеристик інформаційного суспільства, висунутих концепціями інформаційного суспільства – зміни соціальних ролей і ідентичності особистості, а також зміна головних суб'єктів і об'єктів управління, коли місце матеріальних об'єктів зайняли ідеї і символи. Проблеми особистості в інформаційному суспільстві вписані в постмодерністський дискурс. Відповідність постмодерністського світогляду ідеології інформаційного суспільства виразилася в прогностичному осмисленні постмодерністами (перш за все, Ж. Бодрійяром) різноманітності модифікацій людської суб'єктивності в електронно-цифровому середовищі, віртуальній трансформації і симулякризації індивіда, набуття ним свого “віртуального тіла” і актуалізації безлічі комунікативних загроз, які супроводжують заміщення реальності симуляцією і ведуть до електронно-цифрового ескапізму [12].

Однією з базисних характеристик інформаційного суспільства є формування нової людини – “людини інформаційної”. У даній характеристиці важливими стають наступні визначальні моменти. По-перше, значущим є те, якою повинна бути особистість в умовах інформатизації. В умовах розгортання інформатизації кожне з діалектично взаємозв'язаних начал людини: фізичне, психічне й соціальне, вимагає спеціального урахування, оскільки тільки в цьому випадку нові можливості інформаційного суспільства можуть бути повною мірою використані для розвитку людини. Без урахування специфіки цих начал людини, інформатизація загрожує негативними суспільними наслідками.

Сьогодні існує чимало досліджень у найрізноманітніших галузях знань, що присвячено проблемам особистості, які виникають в умовах інформаційного суспільства [13 – 15]. Їх аналіз надає підстав виділити наступні основні соціальні проблеми адаптації людини до мінливих умов інформаційного суспільства:

- проблема мовної комунікації, що становить ядро інформатизації;
- проблема інформаційної безпеки особистості, під якою розуміється стан захищеності інформаційного середовища суспільства, що забезпечує її формування й розвиток на користь громадян, організацій і держави. Проблема забезпечення інформаційної безпеки особистості означає її право на отримання об'єктивної інформації і припускає, що одержана людиною з різних джерел інформація не перешкоджає вільному формуванню й розвитку її особистості.

Впливами на особистість можуть виступати [16, с. 116]:

- цілеспрямований інформаційний тиск з метою зміни світогляду, політичних поглядів і морально-психологічного стану людей;
 - розповсюдження недостовірної, спотвореної, неповної інформації;
 - використання неадекватного сприйняття людьми достовірної інформації.
- Інформаційні впливи є небезпечними або корисними не стільки самі по собі, скільки тим, що управляють могутніми речовинно-енергетичними процесами. Суть впливу інформації якраз і полягає в її здатності контролювати речовинно-енергетичні процеси, параметри яких є на порядок вищими за саму інформацію;

- комп'ютерна злочинність, віруси. Спроба творців вірусів, як правило, молодих людей реалізувати себе у вірусотворчості, пов'язана з низкою причин: бажанням самостверджуватися, “прогриміти”, а також відсутністю усвідомлених життєвих цілей.

Як бачимо, буттєва вкоріненість сучасної людини в інформаційно-технічні детермінанти цивілізаційного розвитку, без сумніву, сьогодні стає актуальною та злободенною проблемою. Соціокультурні виміри інформаційного суспільства також зумовлені виникненням особливого типу автономії особистості: людина може

змінювати свої корпоративні зв'язки, не будучи до них жорстко прив'язаною; вона може і здатна дуже гнучко будувати відносини з іншими людьми, долучатися до різних соціальних спільнот і різних культурних традицій. Світ, який постійно змінюється, обриває численні коріння минулого, змушуючи людину одночасно жити у різних традиціях, культурах, пристосовуватись до перманентно змінних соціокультурних та технічно зумовлених обставин.

У численних наукових працях, присвячених інформаційній ері, здебільшого підкреслюється, що змінюється не тільки технологічна база й інформаційно-технологічні можливості людини, але й сама людина, її самосвідомість. Сучасна людина стає немислимою без інформаційних технологій, які здійснюють величезний вплив на все її існування – як біологічне, так і соціальне. Предметом дискусій стає лише те, що несуть ці зміни.

Сучасні технології, включаючись у середовище суспільних відносин, стають важливим чинником соціальних трансформацій. Крім того, зафіксовані зміни у сфері духовної культури, викликані не свідомими діями її творця – людини, а безособовою логікою технічного розвитку, процесами самоорганізації техногенного середовища. Наприклад, інформаційні технології, за допомогою структуризації інформації й забезпечення її доступності здійснюючи глибокі трансформації індивідуальної й масової свідомості, уніфікують соціальні практики, забезпечують включення людей у глобальний інформаційний обмін і стають інструментом психологічного тиску, насильницьке втручаючись в емоційно-вольову сферу людини. У сучасному інформаційному суспільстві бурхливо поширюються сублімовані форми агресивності. У теперішній час агресія й насильство набули нового вигляду, соціальна агресія стала неминучим та закономірним результатом надмірно тривалого перехідного періоду, що супроводжується розвалом економічних зв'язків, надзвичайно глибоким соціально-економічним розшаруванням населення, регіональними конфліктами, різким падінням рівня життя, кризою моральності. Стало очевидним, що створення загальнопланетарного поля інформації, окрім прискорення взаємообміну культур і їх творчих змін, призводить до розхитування традиційних цінностей [10, с. 126-127].

Наскільки ширшою є сфера застосування технічного, настільки менше аспектів людської діяльності залишаються незалежними від неї. Постійне зростання матеріальних і культурних потреб – причина розвитку промисловості і головний стимул технологічних удосконалень. Але технологічні інновації, крім досягнення своєї прямої мети – підвищення ефективності матеріального виробництва – одночасно розхитують і традиційні основи суспільного життя, і базу традиційної культури. Ці технологічні зміни істотно перетворюють не тільки місце існування людини, але і впливають на саму людину, на організацію всіх видів її діяльності, на взаємини між спільнотами людей на ринку сировини, товарів і послуг, на систему освіти і, нарешті, на норми й закони, що фіксуються і розвиваються законодавчою, судовою і виконавчою владою.

Усе вище сказане свідчить про те, що сьогодні на перший план виходить проблема безпечної адаптації людини в сучасному інформаційному середовищі. Проблема адаптації людини невіддільна від питання про саму її суть, актуальну для філософів у всі часи. Вітчизняні й зарубіжні дослідники неодноразово звертаються до цієї проблематики. Інформаційне середовище, стаючи дедалі більш важливою і невід'ємною частиною навколишнього середовища, висуває до людини зростаючі адаптивні вимоги. Людство було вимушене адаптуватися до природного й штучно створеного інформаційного середовища протягом усього свого розвитку, проте, життя сучасної людини визначається новими реаліями, новими екологічними й соціальними обставинами.

Створення сучасного світового інформаційного простору поступово висуває нові вимоги перед людиною як духовно-суспільною істотою, здатною приймати виклики інформаційної цивілізації і нести відповідальність за власні дії та їх наслідки. Як зазначає Л. Овсянкіна, сучасний світ як система складних і суперечливих глобальних соціально-економічних, політичних, духовних, культурних та інформаційних взаємозв'язків активно підводить людство до вироблення нових цінностей і світоглядних орієнтирів, необхідних для його виживання сьогодні. В епоху, коли руйнуються минулі авторитети і стереотипи, дефіцит духовності може стати серйозною загрозою для подальшого розвитку сучасної цивілізації [17, с. 224].

Розвиток комп'ютерних мереж веде до формування специфічних віртуальних співтовариств, при цьому спостерігаються широка соціальна й культурна диференціація. Важливим антропологічним аспектом стає проблема відчуження, коли пасивне споживання інформації формує жорсткість мислення, позбавляє людей безпосереднього спілкування один з одним, звужує персональний простір, призводить до втрати міжособового спілкування [10, с. 128]. Це призводить до формування класу професіоналів, які, управляючи зв'язками з глобальною економікою, здійснюючи їх сервісне обслуговування й контролюючи розвиток приватного бізнесу, утворюють місцеві суспільства, які живуть у новій інформаційній епосі. Але в цілому “становлення інформаційного суспільства породило канали трансляції соціокультурних норм і цінностей” [10, с. 128], що характерне для появи масової культури, маніпуляції свідомістю людини, що стає могутнім засобом антропосоціогенезу. В результаті культурологічний аспект “мережевої” людини є важливим і сприяє появі на наших очах нового типу культури як культури суспільства епохи інформатизації.

З питання впливу на моральний світ людини мережевої реальності інформаційного суспільства висловлюються діаметрально протилежні точки зору, неначе йдеться про абсолютно різні явища. Оцінки коливаються від визнання світової мережі головним розсадником пороку до віри в можливість вирішення всіх соціальних проблем. Криза традиційних людських форм комунікації необхідно спричиняє собою кризу моральності, оскільки вона за своєю суттю є уявленнями про ідеальні відносини між людьми. За допомогою мережевого простору можна вивчати мови, знайомитися зі світовою культурою, брати участь в інтерактивних конференціях. Іншими словами, перед людиною є вибір: використовувати мережу як розвагу, або з її допомогою займатися власною освітою. І цей вибір залежатиме не від факту наявності Інтернету, а від виховання й соціального оточення людини. На відміну від спілкування людини з технікою, яке носить знеособлений характер і примушує бути такими ж тих, хто ставить своє життя в залежність від подібного спілкування, мережева реальність є місцем прояву яскраво виражених особових якостей.

З цього виходить, що головний вплив на трансформацію людини здійснюють інформаційні й комунікаційні технології. Технологічний розвиток можна розглядати як відхід від початкових умов людського існування. За інформаційними технологіями слідує біотехнології, які вже можуть змінювати нас самих, а не характер наших дій [18]. Як зазначають сучасні українські дослідники, усвідомлення передумов створення біотехнологічних перспектив людини, в яких провідну роль відіграє етика науки й технології – одне з головних питань антропологічної полеміки нашого часу [19 – 22].

Сучасна наука і техніка, зберігаючи загальну установку на перетворення об'єктивного світу, втягують в орбіту людської діяльності принципово нові типи об'єктів, які змінюють тип раціональності й характер діяльності, що реалізується у виробничих і соціальних технологіях. Йдеться про складні системи, що саморозвиваються,

серед яких головне місце займають людинорозмірні, які включають у себе людину як свій особливий компонент. При вивченні людинорозмірних об'єктів пошук істини виявляється пов'язаним з визначенням можливих напрямів перетворення такого об'єкта, що безпосередньо торкається гуманістичних цінностей.

При виявленні майбутніх антропологічних змін, необхідно відзначити етичні наслідки технологічних змін. Як відзначає Е. Фромм: "Людина реагує на зміну зовнішньої обстановки тим, що змінюється сама, а ці психологічні чинники, у свою чергу, сприяють подальшому розвитку економічного й соціального процесу" [23, с. 246].

Виходячи з цього, людина постає перед вибором, який базується на усвідомленні як негативних наслідків "занурення" у простір інформаційного суспільства, так і конструктивних, позитивних можливостей, зумовлених благами такого суспільства.

Проте інтеграція людства й інформаційних технологій здебільшого призводить до негативних наслідків. Наприклад, американський футуролог Е. Тоффлер приводить міркування Д. Міллера про душевне здоров'я людини: "Механізм людської поведінки ламається під дією перевантаження інформацією... але вже зараз, не розуміючи її потенційного впливу, ми збільшуємо швидкості змін в суспільстві. Ми тиснемо на людей, примушуючи їх адаптуватися до нових ритмів життя... ми спонукаємо їх обробляти інформацію з набагато більшою швидкістю. Тому можна не сумніватися, що ми піддамо їх свідомість перезбудженню [24, с. 386].

Таким чином, нова мережева форма організації сприяє становленню нової "мережевої людини", причому комунікації беруть безпосередню участь у формуванні й відіграють вирішальну роль у трансформації такої людини. Перша відмінність нової "мережевої людини" – середовище взаємодії. Людина живе в такому комунікаційному просторі, відмінними рисами якого є відсутність меж, а взаємини відрізняються цілою низкою нових рис і характеристик, які виникають на основі горизонтальних зв'язків. Другою важливою межею в "комп'ютерній людині" М. Кастельса опиняється трансформація простору й часу, яка стала також результатом інформаційної модернізації й розвитку комунікацій. Третьою характеристикою нової "мережевої людини" є втрата ідентичності. Культура "віртуальної реальності" стає фундаментальною четвертою межею нової "мережевої людини". П'ятою відмінністю є гендерні зміни. Основною суперечністю мережевого суспільства, що формується, і людини, є суперечність між глобалізацією світу й ідентичністю конкретної людини, між віртуальним простором і присутністю в ньому малих етнічних і культурних груп, що претендують на збереження ідентичності.

Життєдіяльність сучасної людини реалізується на шляхах все більш активного спілкування з технічними пристроями; якщо раніше вони були як би продовженням людських рук і сприяли посиленню її фізичних потенцій, то виникнення комп'ютера різко змінило положення: він грає роль співробітника, що спільно виконує складну інтелектуальну роботу.

Людина потенційно готова жити і працювати в якісно новому інформаційному середовищі, адекватно сприймати його реалії і, більше того, успішно розвивати його. Таким чином, це змінює не тільки умови життя людини, але і її саму.

Проте, ці зміни носять суперечливий, часом навіть небезпечний характер, що пов'язано з багатьма вельми різноплановими чинниками, наприклад, з необхідністю виділення значних ресурсів суспільства, з неминучою і нерідко хворобливою ломкою різних структур (соціально-економічних, виробничо-технологічних, культурних, чисто інформаційних тощо), з труднощами культурно-психологічної адаптації людини до нетрадиційних інформаційних засобів і технологій. Коротше кажучи, цей процес не можна представляти як суто позитивне явище, без недоліків, витрат і небажаних наслідків.

Один з найсерйозніших моментів, який необхідно враховувати в першу чергу, – можливий негативний вплив новітніх інформаційних засобів і технологій на здоров'я людей, особливо дітей і підлітків. Крім того, зараз, в епоху різкого зростання ролі комп'ютерної техніки, проблема збереження самотності людської особистості набуває особливої важливості як у сфері теоретичного осмислення місця людини в сучасному суспільстві, так і у зв'язку з назрілою необхідністю нових підходів до виховання людини. Існує побоювання, що комп'ютеризація діяльності фахівця, вирішення пізнавальних задач, що не володіє фундаментальною культурою, здатна перетворити людину на придаток машини, позбавити її здатності до творчої діяльності.

Багато дослідників заговорили про виникнення людини нової культури, демонструючи залежність трансформації свідомості від використання абсолютно нового для людської руки інструменту – кнопки. І дійсно, користувач персонального комп'ютера проводить за ним стільки часу і так швидко звикає до механізмів роботи, що можна стверджувати, що кнопка стає новим культурним артефактом.

У світі глобальних інформаційних потоків, неконтрольованого зростання інформаційних ресурсів і необмеженого доступу до них людина стикається з проблемою переробки інформації, вибору необхідної для себе діяльності. І тут комп'ютер не помічник, він може лише видати результат пошуку, але аналіз інформації – завдання людського мислення. А воно не завжди готове до цього вибору, і тоді настає зниження сприйняття й розумових здібностей, а часто й психологічна залежність від нових інформаційних технологій [10, с. 134].

Взаємодія людини й інформаційного середовища здійснює радикальні перетворення і в людській свідомості, вона реалізується на основі вирішення складного завдання розвитку мислення, завдання оперування формальними поняттями і об'єктами. У зв'язку з цим, розвиток комп'ютерної техніки породжує нові парадигми в наукових уявленнях і, відповідно, зміни у звичках і поглядах людей. Нові парадигми формують нове сприйняття людиною свого місця по відношенню до інформаційного середовища і відповідно нове усвідомлення себе та своїх прав і свобод, зокрема інформаційних [26].

Окремо слід виділити проблеми екології людини, пов'язані з бурхливим розвитком інформаційних технологій. В результаті створення людиною нового навколишнього середовища (інформаційного) виникає ситуація, при якій людський організм реагує на зміни середовища появою нових професійних захворювань, хронічною напругою адаптаційних систем. Перераховані проблеми, що виникають в ході взаємодії людини й сучасного інформаційного середовища, вимагають подальшого комплексного осмислення для пошуку оптимальних шляхів їх вирішення.

Висновки.

Таким чином, інформаційне середовище є чинником, що вимагає фундаментально нової адаптації людини. Специфіка сучасного інформаційного середовища веде до корекції існуючих природних і соціальних механізмів адаптації людини і вироблення нових. Інформаційні технології, ставши стрижнем сучасної цивілізації, змінюють не просто якість і зміст життя сучасної людини, вони загрожують трансформувати сам спосіб її буття у світі і безпекові механізми життєдіяльності.

Для інформаційного суспільства характерна велика свобода вибору моделей поведінки людини, в основному за рахунок дистанціювання людей один від одного в процесі життєдіяльності. За умови доступності й відносної легкості і швидкості виробництва інформації, елітарність статусу виробника і розповсюджувача інформації падає, оскільки ним може стати практично будь-який член суспільства, а в ідеалі, інформаційна цивілізація, як і суспільство знання, прагне саме до цього.

Тому підкреслимо, що інформаційне суспільство дійсно стоїть на порозі новітньої історії, і від того, як люди зможуть його сприйняти й інтерпретувати, залежить характер цивілізації майбутнього. Як і будь-який революційний процес, перехід до інформаційного суспільства може мати непередбачувані наслідки. Небезпечний поворот подій є надзвичайно ймовірним, варто лише уявити собі ситуацію монополізації планетарної інформаційної системи або її підпорядкування егоїстичним інтересам окремих груп. Тому проблеми формування інформаційного суспільства, розробки адекватних об'єктивній реальності способів і засобів його життєдіяльності – колективна турбота всього людства.

Використана література

1. Bures V., Otcenaskova T. Complexity of Information Society Achievement of Satisfactory Decision Making. *Postmodern Openings*. 2018. Vol. 9. Issue 2. P. 175-195.
2. Coeckelbergh M. Technology and the good society: A polemical essay on social ontology, political principles, and responsibility for technology. *Technology in Society*. 2018. Vol. 52. P. 4-9.
3. Ramos G., Ruben D., Arevalo T., Maria G. The prevalence of the knowledge society or the information society as structuring elements of the social system. *Prisma Social*. 2018. Issue 20. P. 333-346.
4. Schandl H. Why do we a sociology of society's natural relations to inform sustainable development? *Social Science and Sustainability*. 2017. P. 9-22.
5. Богданова Н.Г. Проблема самореалізації людини у сучасному інформаційному суспільстві. *Гілея: науковий вісник*. 2017. Вип. 126. С. 316-319.
6. Voronkova V., Kyvliuk O. Philosophical Reflection Smart-Society as a New Model of the Information Society and its Impact on the Education of the 21st Century. *Future Human Image-An International Journal for Philosophy, Psychology and Education*. 2017. Issue 7. P. 154-162.
7. Дроздовська О. Взаємодія медіа, Інтернет і людини як фактор вдосконалення інформаційного суспільства: соціально-філософський аналіз. *Гуманітарний вісник Запорізької державної інженерної академії*. 2018. Вип. 73. С. 41-61.
8. Михальчук А.О. Стилi кодування та їх вплив на iнтелект людини в контексті сучасного інформаційного суспільства. *Гілея: науковий вісник*. 2018. Вип. 137. С. 207-211.
9. Тюріна Т.Г. Бездуховність як чинник саморуйнування людини і суспільства (у контексті інформаційно-енергетичної парадигми). *Духовність особистості: методологія, теорія і практика*. 2017. Вип. 3. С. 287-299.
10. Суспільство, людина, право: досвід філософсько-правового осмислення: монографія / О.Г. Данильян, О.П. Дзьобань, С.Б. Жданенко та ін.; за ред. О.Г. Данильяна. Харків: Право, 2018. 350 с.
11. Маклюэн Г.М. Галактика Гутенберга. Становление человека печатающего. Москва: Академический Проект, 2005. 495 с.
12. Бодрийяр Ж. В тени молчаливого большинства, или Конец социального / пер с фр. Екатеринбург: Изд-во Уральского Университета, 2000. 385 с.
13. Дзьобань О.П. Номo informaticus: до проблеми осмислення сутності. *Вісник Національного університету "Юридична академія України імені Ярослава Мудрого". Серія: Філософія, філософія права, політологія, соціологія*. Харків: Право, 2014. № 1 (20). С. 13-21.
14. Кондрусєва В.М. Інформаційне суспільство у контексті сучасної цивілізаційної ситуації (соціально-антропологічний аспект): монографія. Одеса: Бондаренко М.О. 2014. 163 с.
15. Харламов С.Ю. Философско-антропологические модели человека в концепциях информационного общества: дис. ...канд. филос. наук. Белгород, 2009. 166 с.
16. Дзьобань О.П. Філософія інформаційного права: світоглядні й загальнотеоретичні засади: монографія. Харків: Майдан, 2013. 360 с.
17. Овсянкіна Л.А. Філософський аналіз ролі духовних цінностей у розвитку сучасної цивілізації. *Гілея: науковий вісник*. 2012. Вип. 64 (№ 9). С. 224-229.

18. Baranov P.P., Mamychhev A.Yu., Mordovtsev A.Yu., Danilyan O.G., Dzoban A.P. Doctrinal-Legal and Ethical Problems of Developing and Applying Robotic Technologies and Artificial Intelligence Systems (Using Autonomous Unmanned Underwater Vehicles). *National Academy of Managerial Staff of Culture and Arts Herald*. 2018. № 2 (3). P. 465-472.
19. Качак Н. Філософське осмислення буття людини крізь призму сучасних біотехнологій. *Вісник Прикарпатського університету. Філософські і психологічні науки*. 2013. Вип. 17. С. 123-129.
20. Ніколаєнко Н.В. Аксіологічний вимір новітніх біотехнологічних практик. *Вісник Національного технічного університету України "Київський політехнічний інститут". Філософія. Психологія. Педагогіка*. 2012. № 3. С. 42-48.
21. Слободян О.М. Етико-правові проблеми застосування біотехнологій. *Університетські наукові записки*. 2011. № 1. С. 56-63.
22. Терешкун О. Сучасні біотехнології та ідентичність індивіда. *Наукові записки Національного університету "Острозька академія". Серія: Філософія*. 2011. Вип. 8. С. 230-242.
23. Фромм Э. Бегство от свободы / пер. с англ. Г.Ф. Шверника. Москва: Прогресс, 1990. 269 с.
24. Тоффлер Э. Шок будущего / пер. с англ. Е. Руднева и др. Москва: АСТ, 2001. 557 с.
25. Логинов В.А. Интернет: все ли так просто? О психологических проблемах использования сети Интернет в образовании. *Гуманітарні науки*. 2002. № 2. С.154-156.
26. Danilyan O.G., Dzoban A.P., Kalinovsky Y.Y., Kalnytskyi E., Zhdanenko S.B. Personal information rights and freedoms within the modern society. *Informatologia*. 2018. № 51 (1-2). P. 24-33.

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

УДК 342.723

**КОРЖ І.Ф.**, доктор юридичних наук, завідувач науковою лабораторією  
НДІ інформатики і права НАПрН України

## ПРАВО НА ВІДКРИТІ ДАНІ – ЯК ПРАВО ПРИВАТНОГО ХАРАКТЕРУ

**Анотація.** В даній статті досліджуються питання відкритості і прозорості діяльності органів державної влади та органів місцевого самоврядування в частині надання доступу громадськості до відкритих даних. Здійснюється аналіз реальних можливостей здійснення громадського контролю за відкритістю функціонування державних інституцій. Розкриваються недоліки за окремими напрямками здійснення контролю та пропонуються відповідні механізми підвищення його ефективності.

**Ключові слова:** відкриті дані, відкритість, інформація, громадський контроль, прозорість, публічна інформація.

**Summary.** This article examines the issues of openness and transparency of the activities of state authorities and local governments in terms of providing public access to open data. An analysis is made of the real possibilities of exercising public control over the openness of the functioning of state institutions. Shortcomings in certain areas of control are revealed and appropriate mechanisms for improving its effectiveness are proposed.

**Keywords:** information, open data, openness, public information, social control, transparency.

**Аннотация.** В данной статье исследуются вопросы открытости и прозрачности деятельности органов государственной власти и органов местного самоуправления в части предоставления доступа общественности к открытым данным. Осуществляется анализ реальных возможностей осуществления общественного контроля над открытостью функционирования государственных институтов. Раскрываются недостатки по отдельным направлениям осуществления контроля и предлагаются соответствующие механизмы повышения его эффективности.

**Ключевые слова:** информация, общественный контроль, открытые данные, открытость, прозрачность, публичная информация.

**Постановка проблеми.** Однією із ознак демократизації суспільного життя є відкритість і прозорість функціонування органів державної влади, діяльності її посадових і службових осіб, а також відкритість і прозорість прийняття рішень керівником тієї, чи іншої державної інституції. В цьому контексті постає питання відкритості і прозорості бюджетування діяльності керівників державних інституцій різних рівнів, відповідності та адекватності винагороди його праці досягнутим результатам його управлінської діяльності. Не поодинокі факти того, і це висвітлюється в засобах масової інформації, що в суспільстві назріває невдоволення закритості таких питань, коли в підвідомчій сфері того чи іншого керівника державної інституції результати його управлінської діяльності непомітні, однак розмір його заробітної платні не є адекватним досягнутим результатам, що викликає, м'яко кажучи, нерозуміння зазначеного.

**Метою статті** є визначення можливості і доцільності віднесення до статусу відкритої інформації такої інформації, як бюджетне фінансування заробітної платні керівників бюджетних структур, розкриття існуючих проблем, пов'язаних із даним питанням, та напрацювання відповідних пропозицій щодо шляхів їх усунення.

**Виклад основного матеріалу.** Принцип відкритості і прозорості (транспарентності) передбачає відкритість управлінської діяльності органів державної влади та інших державних органів для зовнішнього, насамперед громадського контролю, а прозорість характеризує доступність інформації про діяльність, у тому числі управлінську, органів державної влади та державних управлінських структур. Принцип відкритості став нинішньою реальністю в країнах європейської демократії в 60-х роках минулого сторіччя.

До втілення в життя зазначених принципів проявом відкритості було лише правило опублікування інформації про будь-що в офіційних засобах масової інформації, а впровадження будь-яких адміністративних рішень – після офіційного повідомлення зацікавленої сторони.

В нинішніх умовах, в умовах демократичних перетворень, в умовах запровадження у життя основоположних демократичних управлінських принципів відкритості і прозорості, інформація про стан та результати діяльності державних органів, управлінських структур стали загальнодоступними. Зазначені принципи мають гарантувати здійснення контролю за дотриманням верховенства права у діяльності органів державної влади та інших державних органів, а також їхніх посадових і службових осіб. Зазначене має гарантувати також рівність усіх громадян перед законом і бути необхідною умовою діяльності усіх службовців, оскільки дія згаданих демократичних принципів поширюється на усю публічну сферу, публічну діяльність, публічне управління, і лише законодавчо визначені обмеження в інтересах національної безпеки являється певним правовим обмеженням у її наданні чи поширенні.

Як зазначається у відповідних публікаціях [1], дотримання принципу відкритості і прозорості забезпечує реалізацію двох важливих функцій: захисту інтересів суспільства шляхом підвищення ефективності управління і посилення боротьби з корупцією та є важливим інструментом захисту головної конституційної норми, за якою “людина – основна цінність суспільства” і “джерело влади”. Так, наприклад, публічні адміністрації постійно зобов’язуються повідомляти і обґрунтовувати свої рішення, що допомагає зрозуміти закономірності, яких вони дотримувалися у процесі їх прийняття. А тому відкритість і прозорість діяльності органів державного управління розуміється як можливість людини одержувати інформацію не тільки відносно себе самої (якщо така інформація є в певних організаціях чи установах), а також щодо соціальних, політичних, державних і регіональних питань. Ці два поняття означають відносно необмежений доступ до всіх видів інформації, документів, діяльності і мотивів, а також мають не лише юридичне, а й психологічне та соціальне значення, оскільки втілюють відсутність заборони на оприлюднення інформації та руйнують бар’єр між потребою в інформації і реальним доступом до неї.

Протягом останніх десятиліть у країнах Європейського Союзу докладається багато зусиль для створення відкритої влади. Фахівці, що займаються вирішенням цієї проблеми, вважають, що відкритість влади поєднує три головні елементи:

- прозорість (transparency), іншими словами – перебування під публічним контролем;
- доступність (accessibility) кожному, у будь-який час, всюди;
- чутливість до нових ідей та вимог, готовність оперативно реагувати (responsiveness).

Поняття “відкритість” має ширше значення, ніж широковживаний термін “прозорість”. Відкритість передбачає ще два аспекти – “доступність” та “чутливе реагування”, що є іншими характеристиками якості взаємодії органів влади з громадськістю, якій вона слугує [2, с. 80-98].

Нині більшість європейських дослідників розглядають принципи відкритості і прозорості переважно в рамках концепції “належного урядування”. Розкриття їх змісту в такому контексті має дещо розширений підхід. Підходи європейських учених щодо тлумачення принципів відкритості і прозорості слід поділити на дві групи:

- матеріальний підхід;
- процедурний підхід.

Так прибічник першого підходу професор Каліфорнійського університету Т. Ля Порте вважає, що дотримання принципу відкритості відбувається шляхом забезпечення доступу громадян до відповідної інформації з дотриманням вимог вичерпності та своєчасності її надання [3, с. 53]. Отже, у такому разі мова йде про загальне право громадян на доступ до офіційних документів органів публічної влади та стандарти його належного забезпечення.

Відомий європейський учений М. Галліган зазначає, що адміністративні рішення мають прийматися в умовах максимальної відкритості, яка досягається шляхом відкриття зацікавленим сторонам будь-якої інформації, що стосується адміністративного процесу [3, с. 69]. У даному випадку цей принцип дозволяє сторонам брати участь у процесі прийняття рішення, отримуючи при цьому пояснення й обґрунтування прийнятих рішень.

Які ж позитивні чинники можна відзначити завдяки реалізації принципу відкритості? На нашу думку, ними можуть бути, насамперед, підвищення ефективності діяльності того чи іншого органу при вирішенні завдань, що поставили перед цим органом. Крім того, в діях органу відносно свого персоналу досягаються об'єктивність і справедливість, що зводить до мінімуму прояви для громадян негативних чинників, так само як і для самого органу. Зазначене дозволить підвищити рівень довіри до органу з боку як його працівників, так і населення, яке зачіпають рішення даного органу. Тим самим досягається одна з цілей функціонування демократичного суспільства – здійснення ефективного контролю громадськості за органами влади та адміністративними органами та участі громадськості в управлінні державними та місцевими справами.

У свою чергу принцип прозорості полягає в тому, що державні органи своїми рішеннями і діями створюють умови для залучення громадян до прийняття своїх управлінських рішень.

Таким чином принципи відкритості і прозорості, ефективність правових механізмів їх забезпечення і реалізації є важливою передумовою діяльності органів державної влади в умовах європейської інтеграції України. У зв'язку із зазначеним важливого значення набуває прийняття відповідного законодавчого акту, положеннями б якого забезпечувався ефективний та якісний рівень законодавчої регламентації процедур зовнішньо-управлінської діяльності органів виконавчої влади і органів місцевого самоврядування, їх посадових осіб та інших суб'єктів, які законом уповноважені здійснювати владні управлінські функції, та захист прав і законних інтересів фізичних та юридичних осіб у відносинах із державою.

Таким актом на сьогодні може стати проект Закону про адміністративну процедуру від 28 грудня 2018 року № 9456, внесений Урядом для розгляду Верховною Радою України. Необхідно відзначити, що зазначений законопроект розроблений Міністерством юстиції України на виконання підпункту 1 пункту 22 Плану заходів з реалізації Стратегії реформування державного управління України на 2016 – 2020 роки [4]. Водночас даний законопроект розроблений і внесений на виконання низки інших актів, у тому числі міжнародних. Ними є:

•Рекомендації XIV Третього додаткового звіту про виконання рекомендацій Україною (RC-I/II (2009) 1E), затвердженого Групою держав Ради Європи проти корупції (GRECO) на 59-му пленарному засіданні, яке відбулось 18 – 22 березня 2013 року [5];

•пункту 10 Плану першочергових заходів з подолання корупції [6];

•пункту 13 розділу IV “Заходи з реалізації Плану дій із впровадження Ініціативи “Партнерство “Відкритий Уряд” у 2014 – 2015 роках” [7];

•пункту 69 Плану заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку “Україна – 2020” у 2015 році [8];

•Коаліційної Угоди від 21 листопада 2014 року (протягом I кварталу 2015 року прийняття закону, який врегулює адміністративні процедури) підпункт 2.4 пункту 2 “Реформа публічного адміністрування” підрозділу VII “Децентралізація та реформа публічної адміністрації” розділу А “Реформи” [9].

Необхідність прийняття зазначеного закону викликана тим, що на сучасному етапі розвитку українського суспільства потребують нової оцінки місце і роль держави. Зокрема, положення статті 2 Конституції України [10] проголошують головним обов’язком держави утвердження і забезпечення прав і свобод людини і громадянина, а також встановлюють принцип, згідно з яким саме ці права і свободи та їх гарантії визначають зміст і спрямованість діяльності держави.

Відповідно до положень статті 40 Конституції України [10], усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, які зобов’язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк. А згідно з частиною другою статті 19 Конституції України [10], органи державної влади та органи місцевого самоврядування, їх посадові особи зобов’язані діяти лише на підставі, в межах повноважень та у спосіб, що передбачені Конституцією та законами України.

Як зазначено в пояснювальній записці до законопроекту [11], таким чином держава має гарантувати кожній особі право на неупереджене, чесне вирішення її справи за обґрунтований проміжок часу. Це право повинно включати: право особи бути вислуханою до прийняття будь-якого індивідуального рішення, що може на неї негативно вплинути; право кожної особи на доступ до матеріалів справи, які її стосуються; зобов’язання адміністративних органів обґрунтовувати свої рішення тощо. Зазначені права особи повинні бути закріплені на законодавчому рівні та стосуватися всіх органів виконавчої влади і органів місцевого самоврядування, їх посадових осіб та інших суб’єктів, які законом уповноважені здійснювати владні управлінські функції.

Відповідно до європейських стандартів, визначальною ознакою розвитку законодавства, зокрема адміністративного, є його спрямованість на забезпечення прав і законних інтересів осіб у відносинах із державою та її органами. Однією з найважливіших гарантій цього є чітка регламентація процедурного аспекту відносин особи і влади. За таких умов державний службовець чи службовець органу місцевого самоврядування діє не свавільно, а керуючись чітко встановленим порядком. Це, по-перше, забезпечує рівність осіб перед законом, адже до всіх однопорядкових справ застосовується однакова процедура, а, по-друге, існування законодавчо встановленої процедури є вихідною точкою для здійснення контролю, зокрема судового, за законністю діяльності органів влади.

Ці питання є особливо актуальними для України, оскільки досі більшість процедурних елементів відносин громадян і органів виконавчої влади і органів місцевого самоврядування, їх посадових осіб та інших суб'єктів, які законом уповноважені здійснювати владні управлінські функції, з громадянами або не регулюються законодавством взагалі, або ж регулюються підзаконними нормативно-правовими актами. Отже, необхідність законодавчого регулювання порядку діяльності органів виконавчої влади та органів місцевого самоврядування, їх посадових осіб та інших суб'єктів, які законом уповноважені здійснювати владні управлінські функції, і особливо їх відносин із приватними особами сьогодні не викликає сумнівів.

Отже, адміністративне законодавство України потребує радикального оновлення, результатом якого має стати запровадження нової ідеології функціонування органів виконавчої влади та органів місцевого самоврядування, їх посадових осіб та інших суб'єктів, які законом уповноважені здійснювати владні управлінські функції. Зазначене підтверджується і діями країн-членів Ради Європи, якими прийнято акти, що регулюють адміністративні процедури. Так, зокрема, прийняті Комітетом Міністрів Ради Європи Резолюції [12] та Рекомендації Ради Європи (№ R(80)2 стосовно здійснення дискреційних повноважень адміністративними органами, та № R(87)16 щодо адміністративних процедур, які зачіпають велику кількість осіб та інші)

У більшості європейських країн ефективно діють кодифіковані акти, присвячені детальній регламентації процедур у діяльності органів виконавчої влади та органів місцевого самоврядування в частині їх взаємовідносин з фізичними та юридичними особами. А отже, згаданий законопроект має стати “загальним” нормативно-правовим актом, що запровадить якісно новий рівень законодавчої регламентації процедур зовнішньої управлінської діяльності органів виконавчої влади і органів місцевого самоврядування, їх посадових осіб та інших суб'єктів, які законом уповноважені здійснювати владні управлінські функції, та захисту прав і законних інтересів фізичних та юридичних осіб у відносинах із державою.

Необхідно зазначити, що згаданий законопроект, після його прийняття, разом із Кодексом адміністративного судочинства України мають забезпечувати повноцінну реалізацію один одного, оскільки функціонування окремо один від одного цих актів не є доцільним. Тому згаданий закон мав би бути прийнятим разом із згаданим Кодексом.

Чітке, зрозуміле й очевидне регулювання взаємин людини з публічною владою має неабияку користь, адже кожен знатиме, до чого призведе відхилення від приписів процедурного законодавства. У цьому виявляється стабільність та гарантія забезпечення прав людини. Саме тому така стабільність і впевненість існують у країнах Європи. А якщо законодавство відсутнє або його норми розпорошені по різних законах, суб'єкт владних повноважень може поводитися непередбачувано, що зазвичай має не ті наслідки, на які розраховують громадяни.

Таким чином принцип відкритості передбачає відкритість управління для зовнішніх перевірок, а прозорість характеризує доступність інформації про внутрішню діяльність органів влади. Тому на сьогодні відкритість і прозорість дозволяє кожному дізнатися про механізми прийняття управлінських рішень та створює умови органам нагляду для проведення зовнішніх перевірок. У той же час цей принцип забезпечує обов'язковість чіткого контролю за дотриманням верховенства права, рівності всіх громадян перед законом та є необхідною умовою діяльності службовців на всіх рівнях управління. Адже дія цих принципів поширюється на функціонування всієї системи публічного управління і не стосується лише питань національної безпеки та інформації про особисті дані публічних службовців.

Дотримання принципів відкритості і прозорості забезпечує реалізацію двох важливих функцій: захисту інтересів суспільства шляхом підвищення ефективності управління і посилення боротьби з корупцією та є важливим інструментом захисту головної конституційної норми, за якою “людина – основна цінність суспільства” і “джерело влади”. Так, наприклад, публічні адміністрації постійно зобов’язуються повідомляти і обґрунтовувати свої рішення, що допомагає зрозуміти закономірності, яких вони дотримувалися у процесі їх прийняття. І що важливо, відкритість і прозорість діяльності органів державного управління розуміється як можливість людини одержувати інформацію не тільки відносно себе самої (якщо така інформація є в певних організаціях чи установах), а також, на це акцентується увага, щодо соціальних, політичних, державних і регіональних питань. Ці два поняття означають відносно необмежений доступ до всіх видів інформації, документів, діяльності і мотивів, а також мають не лише юридичне, а й психологічне та соціальне значення, оскільки втілюють відсутність заборони на оприлюднення інформації та руйнують бар’єр між потребою в інформації і реальним доступом до неї.

Таким чином, згадані принципи фактично є каталізаторами підвищення ефективності функціонування органів державної влади та органів місцевого самоврядування у сфері публічного права. Водночас зазначені принципи забезпечують та фактично гарантують доступ громадськості до публічної інформації у формі відкритих даних і тим самим створюють підґрунтя для виникнення відповідного приватного права громадян, тобто свого права мати гарантований доступ до інформації у формі відкритих даних, отримання цих даних, здійснення їх аналізу, обробки і використання. Фактично гарантований доступ громадян до відкритих даних (ст. 10-1 Закону) [13], тобто право на доступ до публічних даних екстраполюється в приватне право на використання цих відкритих даних за власним розсудом громадян, тобто у приватних інтересах.

Відповідно до Закону [13] розпорядники інформації зобов’язані надавати публічну інформацію у формі відкритих даних на запит, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах. Дана інформація є дозволеною для її подальшого вільного використання та поширення. Перелік наборів даних, що підлягають оприлюдненню у формі відкритих даних, вимоги до формату і структури таких наборів даних, періодичність їх оновлення визначаються Кабінетом Міністрів України. При цьому, до такого переліку Кабінет Міністрів України обов’язково включає інформацію, доступ до якої у формі відкритих даних передбачено законом [14].

Створення та забезпечення функціонування єдиного державного веб-порталу відкритих даних здійснюється центральним органом виконавчої влади, що реалізує державну політику у сфері електронного урядування [15]. Оскільки Уряд провадить цілеспрямовану політику в напрямку відкриття найбільш важливих для суспільства наборів даних державних органів, то саме Державне агентство з питань електронного урядування України є державним органом, відповідальним за реалізацію цієї політики. Відкриті дані – це інформація, до якої будь-хто має доступ і яку будь-хто може використовувати і поширювати. Їх використовують як органи влади, так і наукові, дослідницькі, освітні установи, комерційні компанії та громадяни. На основі відкритих даних створюють корисні для бізнесу та суспільства сервіси.

У жовтні 2016 року Україна офіційно приєдналася до Міжнародної хартії відкритих даних, взявши на себе зобов’язання перед міжнародною спільнотою впроваджувати національну політику відкритих даних відповідно до принципів хартії. Хартія являє собою набір принципів і кращих практик для оприлюднення урядових



відкритих даних. Вперше Хартія була офіційно схвалена 17 урядами держав, штатів та міст на Всесвітньому саміті Партнерства “Відкритий Уряд” у Мехіко в 2015 році [16]. Станом на кінець 2018 року, Міжнародна хартія відкритих даних впроваджена 62 урядами й підтримана 57 організаціями. Хартія передбачає 6 принципів для оприлюднення відкритих даних:

- відкритість за замовчуванням;
- оперативність і вичерпність;
- доступність та готовність до використання;
- порівнюваність та інтеоперабельність (англ. interoperability – здатність до взаємодії);
- для кращого врядування та участі громадськості;
- для інклюзивного розвитку та інновацій.

Відкриті дані мають потужний антикорупційний ефект, сприяють прозорості влади, позитивно впливають на розвиток економіки. 2017 року відкриті дані принесли в економіку України понад 700 млн доларів, або 0,67% ВВП. І при збереженні нинішніх темпів, за прогнозами, до 2025 року ця цифра зросте вдвічі – до понад 1,4 млрд доларів, або 0,92 % ВВП [15]. Нині українські відкриті дані увійшли в європейський інформаційний простір і опубліковані на Європейському порталі відкритих даних *europaanddataportal.eu*.

З огляду на зазначене вище, можна констатувати, що гарантування доступу до відкритих даних та їх використання в громадянському суспільстві його членами є з одного боку обов’язком влади, з іншого – правом громадянина, тобто приватним правом. Обмеження на них має визначатися лише через призму національної безпеки. З огляду на це, а також на те, що питання доступу до інформації, ступінь якого разом із розвитком суспільством постійно змінюється, законодавство держави у зазначеній сфері має своєчасно реагувати на зазначену змінність і постійно вдосконалюватися.

Цілком є зрозумілим, що в сучасних умовах впровадження демократичних змін в Україні, питання наповнення відповідним змістом нині законодавчо визначений набір відкритих даних, потребує постійного аналізу, переосмислення та уточнення. Наприклад, відповідно до положень пункту 1 частини першої статті 15 Закону [13], розпорядники інформації зобов’язані оприлюднювати інформацію про організаційну структуру, місію, функції, повноваження, основні завдання, напрями діяльності та фінансові ресурси (структуру та обсяг бюджетних коштів, порядок та механізм їх витрачання тощо). Як видно із наведеного, таке питання, як поводження з бюджетними коштами, не має законодавчих обмежень, окрім пов’язаних із національною безпекою.

Однак, як показує практика, наприклад, таке питання, яке нині є дуже гострим і актуальним для українського суспільства, як заробітна плата, і насамперед керівництва державних інституцій (органів державної влади та органів місцевого самоврядування, інших державних органів та відповідних представників держави), як правило, є відповідним “табу” для більшості громадянського суспільства, незважаючи на фіксацію повідомлень про заробітну плату на сайті електронного декларування. Проблемою є те, що механізм завантаження декларацій є, а механізму їх перевірки немає. Склалася ситуація, коли засобами програмного забезпечення, які є в наявності у НАЗК, можна перевірити лише своєчасність подання декларації, наявність методологічних, логічних та арифметичних помилок. А от достовірність і повноту задекларованих відомостей можна було перевірити лише в ручному режимі за окремими запитами. Як пояснила ситуацію Галина Мельник, юрист ЮФ “Ілляшев та партнери”, одною з основних причин неефективності перевірки електронних декларацій – відсутність нормативної бази для

взаємодії Національного агентства запобігання корупції з іншими структурами, які володіють інформацією, необхідною для перевірки задекларованих показників.

Однак, як свідчать факти, причина такої ситуації не лише у відсутності такого законодавства. Як повідомили “Ні корупції!” у НАЗК, позаминулий рік у Реєстр було подано 1 357 733 декларацій за 2016 рік, станом на 16 березня 2018 року у Реєстр надійшло 595 532 декларації за 2017 рік. При цьому у 2017 році було здійснено повну перевірку 143 декларацій, а у 2018 році перевірили – 77 декларацій. Тому постає питання, яким чином громадянське суспільство зможе проконтролювати грошові витрати державних коштів спрямованих, наприклад, на грошове забезпечення керівників бюджетних інституцій. А підстав для цього є більше ніж потрібно.

Незважаючи на те, що перевірка декларацій покладена на Департамент фінансового контролю та моніторингу способу життя Національного агентства запобігання корупції, продуктивність та ефективність його діяльності бажають бути кращими. Тому, враховуючи ризики для антикорупційної реформи в Україні, низьку якість моніторингу декларацій від НАЗК та пам’ятаючи про міжнародний інтерес до цього питання, презентований в 2018 році ГО “Антикорупційний штаб” посібник з аналізу електронних декларацій посадовців може допомогти залучити більше людей, активістів, студентів, журналістів-розслідувачів та звичайних громадян до процесу моніторингу та перевірки електронних декларацій. Це підтверджується тим фактом, що відповідно до власних перевірок “Антикорупційного штабу”, близько 30 декларацій мають ознаки незаконного збагачення та містять недостовірну інформацію. За результатами перевірок і звернень активістів вже відкрито більше 10 кримінальних проваджень. І це здобутки лише однієї ГО.

На наше переконання, ефективність боротьби з корупцією, ефективність функціонування самих державних інституцій була б вищою і більш відкритою та прозорою за умови дійсно відкритого, прозорого оприлюднення грошових доходів і витрат керівників цих інституцій, які б мали оприлюднюватися на офіційних веб-сайтах цих інституцій.

В чому полягає квінтесенція цієї пропозиції? Головна ідея полягає в тому, що заробітна плата керівництва державної інституції має залежати від результатів їхньої управлінської діяльності, від стану справ на ввіреній їм території, в галузі тощо. Має діяти простий принцип: “Що заробив – те й отримав!”.

Наведемо наступний приклад. В своїй декларації за 2017 рік Євген Кравцов, керівник Укрзалізниці, вказав, що за рік отримав заробітну плату лише в розмірі 157 тисяч грн. Протягом 2018-го року зарплата очільника найбільшої державної компанії суттєво змінилася. Так, лише в березні 2018 року керівник залізниці задекларував оплату праці в розмірі 1 мільйон 205 тисяч гривень. В лютому – 2 мільйони 321 тисячу гривень. Що такого вдатного міг накерувати чи змінити у діяльності Укрзалізниці цей керівник, щоб отримувати таку винагороду? А нічого. Хто користується послугами цієї інституції, особливо у приміському сполученні, може підтвердити, що якихось кардинальних позитивних змін у її діяльності не лише не відбулося, а ситуація навіть погіршилась. Так за що ж отримуються такі захмарні винагороди, за які успіхи вони нараховуються?

На нашу думку, і не лише на нашу, така ситуація – це зловживання службовим становищем, корупція в діяльності керівників державних інституцій, тому що об’єктивних підстав стверджувати про наявні успіхи в управлінській діяльності значної кількості керівного складу державних інституцій, як правило, немає. Тобто, висока грошова винагорода значної кількості керівників державних інституцій не відповідає результатам їхнього напруження. А тому є об’єктивна доцільність забезпечити

залежність рівня грошового забезпечення керівництва державних інституцій від рівня результативності їхнього управлінського напрацювання, яке щомісячно буде зазначатися в засобах масової інформації, включаючи електронні, і буде доступним громадянам відповідного регіону.

Саме громадянське суспільство в умовах демократії має здійснювати контроль за діяльністю керівництва бюджетних структур, оцінювати результати їхньої діяльності, робити у зв'язку з цим відповідні висновки і приймати рішення щодо подальшої їхньої підтримки на відповідній посаді, а за необхідності – їх змінювати.

З огляду на це, пропонується Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних [14], у розділі “Усі розпорядники інформації” доповнити реченням: *Щомісячні дані про заробітну плату керівництва підприємств, установ (закладів) та організацій розпорядника інформації та підпорядкованих йому організацій, що фінансуються з державного чи регіонального або місцевого бюджету.*

Таким чином керівники державних інституцій будуть зацікавлені в позитивному результаті своєї діяльності, від якої буде залежати їхня заробітна плата.

### **Висновки.**

Реальна участь громадськості в управлінні державними справами значною мірою залежить від відкритості і прозорості функціонування державних інституцій, від реальної можливості здійснення громадськістю належного контролю за діяльністю керівництва державних інституцій, за оцінюванням рівня результативності їхньої діяльності в залежності від стану справ на ввіреній їм ділянці чи сфері. Тому пропонується внести зміни в механізм оприлюднення відкритих даних, який би передбачав доступність для громадян відомостей про рівень одержуваного грошового забезпечення керівниками державних установ.

### **Використана література**

1. Економіка. – Муніципальне та державне управління в Україні. URL: <http://economics.studio/derjavne-upravlinnya-munitsipalne/printsip-vidkritosti-prozorosti-78944.html>
2. Дзюндзюк В.Б., Мельтюхова Н.М., Фоміцька Н.В. Публічне адміністрування в Україні: навчальний посібник / за заг. ред. д-ра ф. наук, проф. В.В. Корженка, к.е.н., доц. Н.М. Мельтюхової. Харків: Вид-во ХарPI НАДУ “Магістр”, 2011. 306 с.
3. Susan I. Liem. Constituents of Transparency in Public Administration: With Reference to Empirical Findings from Estonia. Dissertation № 3350. Gutenberg. Schaan. 2007. P. 320.
4. Деякі питання реформування державного управління в Україні: Розпорядження Кабінету Міністрів України від 24.06.16 р. № 747-р. *Урядовий кур’єр*. 27 липня 2016 р. № 139.
5. Третій додатковий звіт про виконання рекомендацій Україною, затверджений GRECO на 59-у пленарному засіданні (Страсбург, 18-22 березня 2013 року). URL: [http://old.minjust.gov.ua/anti\\_corruption\\_grecorep](http://old.minjust.gov.ua/anti_corruption_grecorep) (дата звернення: 22.02.2019).
6. Про затвердження плану першочергових заходів з подолання корупції: Розпорядження Кабінету Міністрів України від 02.07.14 р. № 647-р. *Урядовий кур’єр*. 17 липня 2014 р. № 127.
7. Про затвердження плану дій із впровадження Ініціативи “Партнерство “Відкритий Уряд” у 2014 – 2015 роках: Розпорядження Кабінету Міністрів України від 26.11.14 р. № 1176-р. *Урядовий кур’єр*. 17 грудня 2014 р. № 235.
8. Про затвердження плану заходів з виконання Програми діяльності Кабінету Міністрів України та Стратегії сталого розвитку “Україна-2020” у 2015 році: Розпорядження Кабінету Міністрів України від 04.03.15 р. № 213. URL: <https://zakon.rada.gov.ua/laws/show/213-2015-p> (дата звернення: 22.02.2019).
9. Угода про Коаліцію депутатських фракцій “Європейська Україна”. URL: <https://zakon.rada.gov.ua/laws/show/n0001001-15> (дата звернення: 22.02.2019).

- 
10. Конституція України: Закон України від 28.06.96 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
  11. Про адміністративну процедуру: проект Закону України від 28.12.18 р. № 9456. URL: [http://w1.c1.rada.gov.ua/pls/zweb2/webproc4\\_1?pf3511=65307](http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65307) (дата звернення: 22.02.2019).
  12. Про захист особи відносно актів адміністративних органів: Резолюція (77) 31 Комітету Міністрів Ради Європи від 28 вересня 1977 року. URL: <http://uchebana5.ru/cont/2458299-p78.html> (дата звернення: 23.02.2019).
  13. Про доступ до публічної інформації: Закон України від 13.01.11 р. *Відомості Верховної Ради України*. 2011. № 32. Ст. 314.
  14. Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних: Постанова Кабінету Міністрів України від 21.10.15 р. № 835. *Урядовий кур'єр*. 24 жовтня 2015 р. № 198.
  15. Про затвердження Положення про Державне агентство з питань електронного урядування України: Постанова Кабінету Міністрів України від 01.10.14 р. № 492. *Урядовий кур'єр*. 07 жовтня 2014 р. № 184.
  16. The Open Data Charter: A Roadmap for Using a Global Resource. URL: [https://www.huffingtonpost.com/joel-gurin/the-open-data-charter-a-r\\_b\\_8391470.html](https://www.huffingtonpost.com/joel-gurin/the-open-data-charter-a-r_b_8391470.html) (дата звернення: 24.02.2019).

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

УДК 34.01+351.86(477)+338.22

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

ЦИФРОВИЙ РОЗВИТОК ТА НАЦІОНАЛЬНА БЕЗПЕКА У КОНТЕКСТІ ПРАВОВИХ ПРОБЛЕМ

Анотація. У статті проаналізовано питання державного планування в сфері “цифрової економіки” та розвитку суспільства, досліджено правові проблеми, що виникають у цій сфері. Звернуто увагу на неповне врахування питань забезпечення національної безпеки при державному плануванні. Встановлено, що на загальному рівні поняття “цифровізація” концептуально не відрізняється від загальних явищ інформатизації та побудови інформаційного суспільства. Окреслено відповідне проблемне поле щодо співвідношення права національної безпеки та інформаційного права.

Ключові слова: цифрова економіка, цифровий розвиток, національна безпека, інформатизація, інформаційне право, державне планування.

Summary. This paper analyzes Ukrainian state planning in the digital economy and society development, as well as legal issues arising in this sphere. The lack of consideration to the national security issues in process of state planning are highlighted. Terms “digitalization” and “informatization” are identical in social and legal science. Problematic areas of correlation between national security law and information law are identified.

Keywords: digital economy, digital development, national security, informatization, information law, state planning.

Аннотация. В статье проанализированы вопросы государственного планирования “цифровой экономики” и развития общества, исследованы правовые проблемы, возникающие в этой сфере. Обращено внимание на ситуации неполного учета проблем обеспечения национальной безопасности при государственном планировании. Установлено, что на общем уровне понятие “цифровизация” концептуально не отличается от явлений, характерных для информатизации и построения информационного общества. Выделено соответствующее проблемное поле в соотношении права национальной безопасности и информационного права.

Ключевые слова: цифровая экономика, цифровое развитие, национальная безопасность, информатизация, информационное право, государственное планирование.

Постановка проблеми. Технологічний розвиток, що характеризується карколомною зміною світових трендів, зумовлює відповідне реагування з боку традиційних суспільних інститутів – в першу чергу держави. У вітчизняних реаліях можливо спостерігати активність держави (її органів) у двох основних аспектах – державна підтримка розвитку та державне регулювання відносин. Зазначені аспекти характеризують державну політику і у сфері розвитку інформаційних технологій. Підтримка розвитку знаходить своє відображення у концептуальних документах стратегічного планування (концепціях, стратегіях, доктринах, державних програмах). Державне регулювання відносин, як правило, відбувається шляхом розробки нормативно-правових актів, що регламентуватимуть суспільні відносини. Мета державного регулювання у зазначеній сфері поступово переходить від тотальної регламентації у вигляді дозволів, до іншої крайності – постійного збільшення бази оподаткування шляхом введення додаткових платежів за відсутності інших важелів

реагування. Водночас інтереси забезпечення національної безпеки, незважаючи на постійну декларацію, як правило, при відповідному державному регулюванні не враховуються.

Оновлення вітчизняного законодавства у сфері національної безпеки та в інформаційній сфері відбувається мало пов'язаними паралельними шляхами. За таких умов не досягається мета правового регулювання, а державне (стратегічне) планування має мало спільного з реальністю. Доволі складно диференціювати справжні наміри належного адекватного регулювання від заходів, спрямованих на отримання публічної підтримки політиків та політичних утворень. Численні напрацювання фахівців у сфері державного управління, корпоративного планування, інформаційних технологій, які враховуються при розробці відповідних документів стратегічного планування, розглядають проблему забезпечення безпеки суто в технічному ракурсі переважно як захист інформації, хоча трансформація загроз на сьогодні є досить широкою.

“Цифровізація” (“цифрова економіка”), що є останнім технологічним трендом, який зумовлює активність у сфері державного планування, є предметом деяких основних документів стратегічного планування, ухвалених останнім часом на рівні Кабінету Міністрів України, тому важливим є дослідити зазначені новації на предмет врахування усього комплексу сучасних викликів та загроз, у першу чергу в сфері національної безпеки та оборони. Останніми роками і поява новітніх технологій в інформаційній сфері зумовила зростання суспільного (а в подальшому – рекламного і політичного) інтересу та трансформацію окремих документів державного планування.

Результати аналізу наукових публікацій. Проблеми державного управління у сфері розвитку інформаційних технологій досить детально розглядаються в економічному, управлінському, політологічному контексті. У правовій науці можливо спостерігати вельми вузьке розуміння зазначених проблем – в рамках відповідних галузей правової науки. Диференціація на окремі галузі і встановлення між ними бар'єрів (що традиційно склалось у вигляді чіткої відповідності дисертаційних досліджень визначеним паспортам спеціальностей) не сприяє комплексному розгляду питань правового регулювання. Якщо проаналізувати існуючий масив публікацій з цього приводу, то мова йде насамперед про ще одне адміністрування (адміністративно-правові аспекти регулювання певної сфери – у даному випадку застосування технологій), або у вирішенні конкретних казусів (що характерно для цивільно-правової науки). Безпекова проблематика розглядається або у контексті нормативного забезпечення захисту інформації, або в контексті протидії комп'ютерній злочинності. Комплексні дослідження останнього часу, що враховують розвиток новітніх технологій, характерних для так званої “цифрової епохи”, є доволі нечисленними [1 – 5], але вони створюють наукову базу для подальших ґрунтовних розробок.

Метою статті є аналіз стану державного планування у сфері “цифровізації” (“цифрової економіки”) та пов'язаних сферах новітніх інформаційних технологій (у першу чергу технологій розподілених реєстрів) у розрізі врахування загроз національній безпеці та побудови відповідних механізмів протидії, виокремлення проблемного поля правового регулювання і практичного застосування норм права.

Виклад основного матеріалу. Розпорядженням Кабінету Міністрів України від 17.01.18 р. № 67-р схвалено Концепцію розвитку цифрової економіки та суспільства на 2018 – 2020 роки. Зазначений документ передбачає здійснення заходів “щодо впровадження відповідних стимулів для цифровізації економіки, суспільної та соціальної сфер, усвідомлення наявних викликів та інструментів розвитку цифрових інфраструктур, набуття громадянами цифрових компетенцій, а також визначає критичні

сфери та проекти цифровізації, стимулювання внутрішнього ринку виробництва, використання та споживання цифрових технологій” [6].

Розуміння терміну “цифровізації” наведено у тій же Концепції як “насичення фізичного світу електронно-цифровими пристроями, засобами, системами та налагодження електронно-комунікаційного обміну між ними, що фактично уможлиблює інтегральну взаємодію віртуального та фізичного, тобто створює кіберфізичний простір” [6]. Зазначене визначення є суто філософським і навряд чи його може бути безпосередньо імплементовано в право. Водночас його можливо враховувати на світоглядному рівні у подальшому, хоча подібна концепція відома у технічних колах досить давно. Свого часу В.М. Глушков, розглядаючи сутність “безпаперової технології”, зазначав, що зберігання інформації в пам’яті електронно-обчислювальних пристроїв та налагодження безпосередньої взаємодії між ними завжди вимагає присутності людини, як суб’єкта цієї системи [7, с. 13]. У подальшому питання “безпаперовості” (у значенні повної чи часткової відмови від зберігання інформації на паперових носіях) розглядалось у концепціях “електронного” (“віртуального”, “кібернетичного”) урядування, документообігу тощо. У випадку використання певних технологій стосовно існуючих феноменів – комерції, управління, демократії створюється нове модифіковане явище – “електронна” комерція, уряд, демократія [8, с. 78-79, 81, 96-97], а у випадку ведення інформаційної війни у мережах – електронна боротьба [9, с. 14].

На нашу думку суть “цифровізації” можливо викласти більш коротко, аніж у тексті Концепції, ґрунтуючись на співвідношенні термінів “оцифрування” та “цифровізація”.

У першому випадку мова йде про перенесення інформації на цифровий (безпаперовий) носій, у другому – про створення інформаційного продукту у віртуальному середовищі, при цьому його перенесення на паперовий носій неможливе без втрати якості (змісту) [10, с. 8].

Отже, обране у тексті Концепції значення для терміну “цифровізація” є не досить вдалим з огляду на характер явища, яке вона намагається описати. Як вбачається, основним предметом регулювання у Концепції є все ж саме “цифрова економіка”, термін, що відомий з 1995 року. Його відмінність від “електронної торгівлі”, “електронного банкінгу” полягає в тому, що мова йде про створення продуктів, послуг безпосередньо в мережі Інтернет, а не застосування інформаційно-комп’ютерних технологій до традиційної торгівлі, банківських, страхових послуг.

Іноді різниця мало відчутна. Популярні на сьогодні “мережеві боти”, як послуга, є спеціальною віртуальною програмою, але у багатьох випадках вона пов’язана із традиційною діяльністю – “патент-боти” автоматично заповнюють реєстраційні форми і здійснюють реєстрацію, “юридичні боти” автоматично складають документи визначеної процесуальної форми і направляють їх адресатам тощо.

Концепції розвитку цифрової економіки розроблялись різними країнами починаючи з кінця 1990-х і містили у собі перелік заходів державного управління, підтримки окремих видів економіки, подолання технологічних, організаційних, правових, культурних бар’єрів тощо.

Мета вітчизняної Концепції розвитку цифрової економіки та суспільства на 2018 – 2020 роки визначена доволі широко. Зокрема, її цілями є:

- прискорення економічного зростання та залучення інвестицій;
- трансформація секторів економіки в конкурентоспроможні та ефективні;
- технологічна та цифрова модернізація промисловості та створення високотехнологічних виробництв;

- доступність для громадян переваг та можливостей цифрового світу;
- реалізація людського ресурсу, розвиток цифрових індустрій та цифрового підприємництва [6].

Як правило, мету стратегічного планування розвитку цифрової економіки на національному рівні викладають простіше. Свого часу Уряд Австралії, ухваливши у 2010 році Національну стратегію цифрової економіки, визначив її як досягнення рівня лідерів цифрової економіки [11]. Метою Стратегії цифрової економіки на 2015 – 2018 роки, ухваленої Урядом Великої Британії є “допомогти вітчизняному бізнесу здійснити інновацію за допомогою цифрової економіки” [12].

Не зупинившись на основних цілях, розробники вітчизняної Концепції визначили ще й головну мету, як “реалізацію прискореного сценарію цифрового розвитку, як найбільш релевантного для України з точки зору викликів, потреб та можливостей” [6], а також досягнення певних конкретних місць для країни у міжнародних рейтингах.

Деталізуючи такі цілі, розробники Концепції визначили низку принципів. При цьому проблем безпеки стосується принцип 7, що визначається наступним чином: “інформаційна безпека, кібербезпека, захист персональних даних, недоторканність особистого життя та прав користувачів цифрових технологій, зміцнення та захист довіри у кіберпросторі є, зокрема, передумовами одночасного цифрового розвитку та відповідного попередження, усунення та управління супутніми ризиками” [6]. Серед змістовної частини принципу два носять загальний характер – інформаційна та кібербезпека, а решта – стосується лише прав приватних осіб (персональні дані та приватність). Таким чином, національна безпека не розглядається авторами Концепції як окремий принцип. Окремо у тексті Концепції визначається напрям громадської безпеки як протидії злочинності.

Розроблений на виконання Концепції план заходів містить 38 пунктів, що стосуються конкретних напрямів цифровізації та розвитку цифрової економіки. Водночас, концептуально нові підходи, які запроваджені у державному плануванні зумовлюють певні складнощі з огляду на загрози національній безпеці та протидію агресії проти нашої держави. У п. 33 Концепції передбачено розроблення плану заходів із стимулювання та підтримки запровадження технології блокчейн у сфері державного управління та інших сферах. Таким чином, акцентовано увагу на необхідності державної підтримки застосування саме технології блокчейн.

Оскільки сам по собі “блокчейн” у сучасному світі є активним трендом, який досить широко використовується у медійному середовищі та літературі, що відзначалось у правових дослідженнях [2, с. 65, 69], досить цікаво визначити, які саме механізми обере держава і які галузі застосування технології розглядаються. По-перше, визначення у тексті Концепції блокчейну як “програмно-комп’ютерного алгоритму децентралізованого публічного або приватного реєстру чи бази даних, функціонування якої забезпечується шляхом взаємодії через Інтернет однорангової мережі, або будь-яким іншим способом, що гарантує належний криптографічний захист усіх записів, транзакцій, проведених з використанням відповідної технології” [6] є невдалим. Хоча б з тієї причини, що блокчейн розуміється спочатку як алгоритм, а в Плані заходів як технологія.

У рамках даної статті неможливо висвітлити відповідну дискусію, але розуміння блокчейну як алгоритму не дозволяє ефективно оперувати зазначеним терміном, визначаючи конкретні заходи. Якщо мова йде про державне регулювання, підтримку, реалізацію в певних сферах та про правові проблеми, блокчейн розуміється саме як технологія. Так, сучасні дослідники соціальних та правових проблем блокчейну,

визначаючи його суть на технічному рівні подібно до розробників Концепції, у подальшому ведуть мову про “блокчейн-технології”, або про технології на основі блокчейн [13, с. 136].

На нашу думку необхідно також більш широко розглядати технології, що можуть застосовуватись в інтересах довіри, зокрема мова повинна йти не про суто блокчейн, а про технології розподілених реєстрів (DLT), що вже було зазначено автором свого часу [14, с. 53]. Тим більше, що DL-технології, які не є блокчейном, застосовуються досить широко у цифровій фінансовій сфері (fintech).

Вченими, що досліджували проблему використання технології на основі блокчейн в публічному праві, цілком вірно визначено основні проблемні моменти, що стосуються правової регламентації застосування технологій [2; 3]. Окрім цього варто звернути увагу і на існуючий в державі правовий механізм захисту інформації.

На сьогодні чинним є Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 05.07.94 р. № 80-94ВР з відповідним змінами і доповненнями [15]. Зазначений Закон визначає об’єкти, суб’єкти відносин, порядок доступу до інформації, умови обробки інформації, забезпечення її захисту, відносини між суб’єктами та повноваження державних органів. На прикладі застосування блокчейн-технологій до ведення державних реєстрів можливо визначити, що юридично вона взагалі не може бути застосована до інформації, яка підлягає захисту, з огляду на те, що неможливо визначити, хто є власником системи у розумінні приписів вказаного Закону. На прикладі застосування новітніх технологій до певних видів державних реєстрів можливо визначити, що технічні можливості доступу до технології де-факто надають іноземні юридичні особи. У межах наукової статті немає потреби розглядати відповідні журналістські розвідки з цього приводу, але суспільні питання стосовно обрання належних суб’єктів виникають з огляду на неоднозначну репутацію окремих компаній та осіб, що запропонували свої послуги [16; 17]. Підстав вважати, що інформація з державних реєстрів може бути відкритою у будь-якому випадку наразі немає оскільки вона обов’язково міститиме персональні дані.

Таким чином, на прикладі “блокчейн-технологій” можливо відразу визначити складнощі у втіленні технологій з огляду на вимоги законодавства стосовно захисту інформації. При цьому його комплексне оновлення прямо не визначено серед заходів, які запропоновані розробниками Концепції.

На сьогодні групою фахівців при Міністерстві економічного розвитку і торгівлі України розробляється інший концептуальний документ (“Цифрова адженда 2020”), що презентований як версія 1.0. Не позбавлений декларативності, цей документ визначає аналогічні цілі, ґрунтуючись на так званій “цифровізації”, у значних обсягах вводять нові терміни-кальки (диджиталізація тощо) [18]. На рівні конкретних заходів передбачено низку стимулюючих методів. Водночас стосовно безпеки автори бачать лише поле для застосування певних технологій в інтересах громадської безпеки та боротьби зі злочинністю.

Отже, можливо констатувати єдність підходів розробників концептуальних документів розвитку цифрової економіки, у тому числі широке сприйняття зазначеної проблематики і намагання охопити практично усі суспільні сфери.

Зазначені проблеми безумовно здійснюють вплив на забезпечення національної безпеки і тому мають враховуватись при відповідних заходах, спрямованих на належне правове регулювання. Актуальні загрози національній безпеці України визначено Стратегією національної безпеки України, затвердженою Указом Президента України від 26.05.15 р. № 287/2015 [19]. Основними з них є ті, що пов’язані із агресією проти

нашої держави. У контексті питань, що розглядаються доцільно було б визначити наступні блоки загроз:

- розвідувально-підривна і диверсійна діяльність, дії, спрямовані на розпалювання міжетнічної, міжконфесійної, соціальної ворожнечі і ненависті, сепаратизму і тероризму;

- торговельно-економічна війна;
- інформаційно-психологічна війна.

Перший блок загрози може бути прямо пов'язаний із технологіями, оскільки мова йде про збереження у державних реєстрах критично важливої інформації. І у даному випадку існуючий законодавчий порядок захисту інформації має бути дотриманий при будь-якому переводі реєстрів на інші носії.

Інші блоки можуть бути пов'язані із застосуванням маніпулятивних технологій. Визначені у літературі способи маніпулювання свідомістю [9, с. 44] цілком трансформуються в епоху технологій – від традиційних друкованих засобів масової інформації до новітніх соціальних мереж. Існуючі законодавчі засоби протидії в умовах сучасного світу є неефективними. Наприклад, можливо заборонити розповсюдження на території держави друкованої продукції (відома заборона ввезення та продажу, що здійснюється відповідно до компетенції державним органом), але стосовно отримання оцифрованих копій такої ж продукції юридична заборона не діє. Блокування певних Інтернет-ресурсів (у першу чергу електронної торгівлі) також не досягає цілей, оскільки розвиваються нові технології розповсюдження інформації (хоча б на основі р2р). На цей час досить складним питанням є протидія інформаційно-психологічним впливам та їх проявам оскільки існуючі заходи блокування доступу до інформації далеко не завжди є ефективними.

Сама по собі згадувана вище блокчейн-технологія повинна досить обережно застосовуватись при зберіганні інформації державних реєстрів, можливо, більш доцільним було б використати в існуючих системах її криптографічну складову (на рівні протоколів). До того ж необхідно комплексне та ґрунтовне вирішення питання оновлення законодавства щодо захисту інформації в інформаційно-телекомунікаційних системах.

Окрім цього, слід визначити і співвідношення державного стимулювання та можливості державних обмежень у цій сфері. Наприклад, для розвитку будь-якої економіки (у тому числі для “цифрової економіки”) важливою є передбачуваність. У такому разі обмежувальні заходи відповідно до Закону України “Про санкції” мають застосовуватись за чітким та прозорим механізмом, інакше вони становитимуть загрозу розвитку економіки. Прикладом цього є прийняття рішення про фактичне блокування Інтернет-ресурсів з посиланням на п. 25 ч. 1 ст. 4 зазначеного Закону України, яка передбачає можливість застосування “інших санкцій” окрім уже перелічених у попередніх 24 пунктах цієї статті [20]. Поряд з окресленими можливо виникнення нових непередбачуваних правових проблем, пов'язаних із застосуванням законодавства у сфері національної безпеки і оборони до відносин, які виникають при впровадженні новітніх технологій.

Досить ґрунтового аналізу потребують і заходи, пов'язані із суто технічними питанням впровадження широкосмугового доступу до Інтернету, зменшення вартості використання мережі Інтернет, тощо, з огляду на стан правового регулювання використання ресурсів, телекомунікацій тощо. Окрім цього, привертає увагу принцип 6 Концепції розвитку цифрової економіки та суспільства на 2018 – 2020 роки, що стосується стандартизації, проголошуючи неприпустимість (за винятком сфери оборони

та безпеки) побудови цифрових систем лише на українських стандартах. Зазначений принцип також має бути застосований лише на підставі досить ретельного правового аналізу питань стандартизації.

Висновки.

Викладене вище дозволяє визначити наступне.

1. Термінологічне визначення “цифровий” стосовно відносин, суспільства та його окремих інститутів не містить нового змісту порівняно з тими, що вживались до опису ідентичних процесів у минулому (“електронний” та ін.), за винятком “цифрової економіки”, яка полягає у виробництві та продажу товарів та послуг, які не існують у фізичному світі, але використовуються людьми.

2. Державна підтримка у цій сфері перебуває на початковому етапі. Розроблено концептуальні документи, що спрямовані на надання відповідних переваг та інших стимулюючих заходів з метою розвитку відповідного сектору вітчизняної економіки. Водночас задекларовані на концептуальному рівні цілі потребують ретельного правового аналізу з огляду на існуючий стан правового регулювання та правозастосовчої практики.

3. Питання нейтралізації загроз національній безпеці враховано при розробці відповідних концепцій та документів стратегічного планування дещо побіжно. Окремі технології, підтримка яких задекларована, вочевидь несуть реальні та потенційні загрози.

4. Законодавча та нормативно-правова база, що склалась у сфері захисту інформації, потребує певного оновлення, але лише на підставі ретельного аналізу суті та перспектив розвитку технологій та їх впливу на суспільні загрози. Важливим є врахування необхідності забезпечення національної безпеки в умовах протидії агресії проти нашої держави.

Використана література

1. Жилиєв І.Б., Семенченко А.І., Фурашев В.М. Інструменти державного стратегічного управління: національна програма інформатизації. *Інформація і право*. № 1(24)/2018. С. 44-58.
2. Баранов О.А. Інтернет речей (IoT) і блокчейн. *Інформація і право*. № 1(24)/2018. С. 59-71.
3. Радейко Р.І. Особливості впровадження технології блокчейн у сфері публічних відносин в Україні. *Часопис цивілістики*. 2018. Вип. 29. С. 112-118.
4. Доронін І.М. Розвиток емерджентних (новітніх) технологій та регулювання у цій сфері як реалізація функцій держави. *Інформація і право*. № 4(23)/2017. С. 41-48.
5. Чукут С.А., Буряченко К.О. Блокчейн чи система електронного документообігу: сучасні тенденції впровадження в органах виконавчої влади України. *Інвестиції: практика та досвід*. 2018. № 1. С. 70-76.
6. Концепція розвитку цифрової економіки та суспільства на 2018 – 2020 роки: Розпорядження Кабінету Міністрів України від 17.01.18 р. № 67-р. *Урядовий кур'єр*. 11.05.2018. № 88.
7. Глушков В.М. Основы безбумажной информатики. Изд. 2-е, испр. Москва: Наука, 1987. 552 с.
8. Фурашев В.М., Ланде Д.М., Григор'єв О.М., Фурашев О.В. Електронне інформаційне суспільство України: погляд у сьогодення і майбутнє: монографія. Київ: Інжиніринг, 2005. 164 с.
9. Брижко В.М. та ін. е-боротьба в інформаційних війнах та інформаційне право: монографія. Київ: НДЦПІ АПРН України, 2007. 239 с.

10. Андреева Г.Н. и др. Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография. Нижний Новгород: Профессиональная наука, 2018. 131 с.
11. Australian Government National Digital Economy Strategy: 2010. URL: http://rdanwq.org.au/files/National_Digital_Economy_Strategy.pdf (Last assessed 12.01.2019).
12. Innovate UK: Digital Economy Strategy 2015-2018. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/404743/Digital_Economy_Strategy_2015-18_Web_Final2.pdf (Last assessed: 12.01.2019).
13. Reijers W., O'Brolchain F., Haynes P. Governance in Blockchain. Technologies & Social Contract Theories. *Ledger*. 2016. № 1. P. 134-151.
14. Доронін І.М. Використання сучасних технологій розподіленої обробки даних: право та функції держави. *Інформація і право*. № 2(21)/2017. С. 51-58.
15. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.94 р. № 80-94ВР. Дата оновлення: 19.04.2014. URL: <https://zakon2.rada.gov.ua/laws/show/80/94вр> (дата звернення: 13.01.2019).
16. Stack Graham. Bitcoin miner steps out into the light. *New Business Europe*. 2015. August. P. 34-36.
17. Начало грандиозной аферы: коррупцию переводят на блокчейн. *CrimeUA*. 22.03.2018. URL: <http://crime-ua.com/node/23088>
18. Цифрова адженда 2020. Концептуальні засади. Версія 1.0. URL: <https://uccr.org.ua/uploads/files/58e78ee3c3922.pdf> (дата звернення: 03.01.2019).
19. Про рішення Ради національної безпеки і оборони України від 6.05.15 р. “Про Стратегію національної безпеки України”: Указ Президента України. *Офіційний вісник Президента України*. 2015. № 13. Ст. 874.
20. Про санкції: Закон України від 14.08.14 р. № 1644-VII. Дата оновлення: 17.12.2017. URL: <https://zakon.rada.gov.ua/laws/show/1644-18> (дата звернення: 21.01.2019).

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

УДК 340:004

**ТИХОМИРОВ О.О.**, кандидат юридичних наук, доцент,  
доцент кафедри цивільно-правових дисциплін,  
Національна академія Служби безпеки України

## ІНФОРМАЦІЙНИЙ ДЕЛІКТ ЯК ПІДСТАВА “ІНФОРМАЦІЙНОЇ” ЮРИДИЧНОЇ ВІДПОВІДАЛЬНОСТІ: ВІДМІТНІ ОЗНАКИ

**Анотація.** У статті розглянуто ознаки, за якими інформаційні делікти може бути виокремлено серед інших видів правопорушень. Визначено, що ключові відмітні юридичні ознаки інформаційних деліктів стосуються їх об'єкта і об'єктивної сторони. Надано деякі пояснення ознак у взаємозв'язку інформаційного делікту з юридичною відповідальністю.

**Ключові слова:** інформаційний делікт, інформаційна деліктологія, склад інформаційного делікту, юридична відповідальність за інформаційний делікт.

**Summary.** The article deals with the features by which information delicts can be distinguished among other types of offenses. It is determined that the key distinctive legal features of information delicts characterize their object and objective side. Some explanations of the relationship of the information delict and information responsibility are given.

**Keywords:** information delict, information delictology, information delict composition, legal liability for information delict.

**Аннотация.** В статье рассмотрены признаки, по которым информационные деликты можно выделять среди других видов правонарушений. Определено, что ключевые отличительные признаки информационных деликтов касаются их объекта и объективной стороны. Представлено некоторые пояснения признаков во взаимосвязи информационного деликта с юридической ответственностью.

**Ключевые слова:** информационный деликт, состав информационного деликта, информационная деликтология, юридическая ответственность за информационный деликт.

**Постановка проблеми.** Категорія “правопорушення в інформаційній сфері” привертає увагу багатьох вітчизняних науковців. З одного боку, є об'єктивні причини такої актуальності, пов'язані зокрема з критичним станом інформаційної безпеки України, наслідки якого спостерігаються щодня, а з іншого, – це “мода” у вітчизняній юридичній науці на недостатньо досліджену інформаційно-правову тематику, в межах якої багатьом дослідникам простіше просувати власні здобутки, які претендують на наукову новизну, і таким чином виконати кваліфікаційні вимоги підготовки науково-педагогічних кадрів. Водночас, розвиток інформаційно-правової думки, вкрай необхідний Україні, вимагає особливо виважених і прагматичних наукових позицій, що якомога скоріше приведуть до реального втілення вироблених ідей в практичну юриспруденцію і загалом у життя українського суспільства.

Зрозуміло, що належне юридичне реагування на різні правопорушення є одним з пріоритетів функціонування правової системи, тому їх дослідження завжди затребувані. Інформаційні правопорушення, які вже набули у вітчизняному інформаційному просторі системного характеру, – одне з найнебезпечніших для сучасної України явищ. Тому їх ефективне вивчення та адекватне подання відповідних наукових результатів можливе тільки в межах розвитку комплексного напрямку знань – інформаційної деліктології, чому присвячена зокрема ця стаття.

**Результати аналізу наукових публікацій.** Інформаційно-правова наука в Україні наразі активно розвивається, але вже має власну доктринальну основу. Її фактично створено роботами відомих українських учених, серед яких І.В. Арістова, О.А. Баранов, К.І. Беляков, Б.А. Кормич, О.В. Кохановська, Т.А. Костецька, А.І. Марущак, О.Д. Тихомиров. Разом із тим, концептуальні проблеми правопорушень в інформаційній сфері та особливостей відповідальності за них є предметом наукових публікацій О.А. Заярного, Л.П. Коваленко, В.К. Колпакова, Ю.Є. Максименко, В.Я. Настюк, А.А. Письменицького, С.М. Правдюка, О.М. Селезньової та інших. При цьому нерідко науковців особливо приваблює концепт “інформаційне правопорушення – інформаційна відповідальність”, який, щонайменше, потребує переконливої аргументації. Але, і щодо тлумачення інформаційного правопорушення та його типізації, і щодо обґрунтування виділення для “інформаційної відповідальності” загальновизнаних сталих позицій у вітчизняній правовій науці ще не сформувалося.

**Метою статті** є виділення та характеристика ключових ознак інформаційних деліктів, що мають безпосереднє юридичне значення, як компоненту знань інформаційної деліктології і засад формування й розвитку інституту “інформаційної” юридичної відповідальності.

**Виклад основного матеріалу.** Розгалуженість сучасної юриспруденції, її складний дослідницький арсенал, зумовлюють значну варіативність можливих підходів до інформаційних деліктів, зокрема їхніх ознак, рис, властивостей, видів, що загалом становлять онтологічні й гносеологічні основи інформаційної деліктології. Тому сукупність характеристик інформаційних деліктів, отриманих в результаті пізнання в межах тієї чи іншої юридичної діяльності, завжди зумовлюються галуззю юриспруденції, її предметною сферою, метою і завданнями, методологічною основою тощо. Наведемо деякі приклади.

Так, осмислюючи юридичну природу інформаційних правопорушень, С.М. Правдюк виокремлює низку ознак, які по суті є відмітними: міжгалузевий характер; ідеальний характер; вчиняються, як правило, в інформаційній сфері, середовищі; складність ідентифікації правопорушника, джерела небезпеки, місця і часу вчинення; динамічний та перманентний розвиток способів, засобів вчинення; тощо [1, с. 8-9]. Загалом підтримуючи обґрунтованість думок С.М. Правдюка, які відповідно до спрямованості його досліджень мають загальнотеоретичний характер, необхідно зазначити, що не всі запропоновані ознаки інформаційних правопорушень будуть однаково важливими в контексті юридичної відповідальності за такі порушення, і, відповідно, у світлі завдань цієї статті.

За іншого підходу, дослідники пропонують всю сукупність ознак правопорушень в інформаційній сфері диференціювати на: 1) загальні – соціального, юридичного, об’єктивного, психологічного, наслідкового характеру; 2) спеціальні – ознаки предметного характеру і ознаки інформаційної складової об’єктивної сторони інформаційного правопорушення. При цьому спеціальні ознаки виступають як відмітні для правопорушень цього виду [2, с. 144]. Такий розподіл також можливий, але є доволі умовним через неоднорядковість виділених характеристик.

Очевидно, що варіантів авторських наукових позицій щодо явищ “інформаційний делікт”, “інформаційне правопорушення”, “правопорушення в інформаційній сфері” може бути багато. На шляху формування доктринальних інформаційно-деліктологічних знань, найбільш доцільним видається виділення правових ознак, які орієнтують на осмислення своєрідної інформаційності правопорушення та встановлення місця інформаційних деліктів в системі правової поведінки загалом та протиправної зокрема.

Інформаційні делікти в широкому розумінні (правопорушення в інформаційній сфері) мають подвійне походження – як власне інформаційне, так і інше, притаманне тим деліктам, які завдяки розвитку ІТ набули нового інструментарію вчинення [3]. У зв'язку з цим, іманентні ознаки інформаційних деліктів виявляються в єдності загального і своєрідного в їхній правовій природі.

У процесі розгляду інформаційних деліктів, властиві їм ознаки можуть комбінуватися залежно від вирішуваних завдань наукової, освітньої чи практичної юридичної діяльності, зокрема як:

*ознаки науково-пізнавального характеру* – виділені в процесі наукового осмислення, узагальнення, спроб систематизації, виявлення нового, спільного і відмітного порівняно з іншими деліктами тощо, що необхідно для виконання конкретних завдань певних наукових досліджень;

*загально-правові ознаки* – інтерпретовані в результаті розгляду інформаційних деліктів крізь призму традиційної конструкції правопорушення в теорії права, що може використовуватися з навчально-пізнавальною метою;

*формально-юридичні ознаки* – відображені (змодельовані) в елементах складу окремих правопорушень, передбачених законом;

*фактичні ознаки* – характеристики конкретних вчинених інформаційних деліктів, які є предметом охоронної правозастосовної практики і відповідного юридичного аналізу.

Із наведеного вище останні дві групи ознак мають особливе значення в контексті формування нормативно-правових засад “інформаційної” юридичної відповідальності та її практичної реалізації. Причому йдеться не про окремі компоненти юридичної відповідальності суто інформаційного характеру, як то обмеження можливості здійснювати певну інформаційну діяльність, що, наприклад, А.А.Письменицький називає інформаційно-правовою відповідальністю [4, с.115], а про комплексний інститут юридичної відповідальності, який охоплює механізми, санкції, засоби, заходи що застосовуються за правопорушення в інформаційній сфері і можуть мати різну галузеву приналежність.

Правопорушення в інформаційній сфері, як і будь-які інші правопорушення, мають ознаки об'єктивного і суб'єктивного характеру. Але оскільки нові категорії суб'єктів правопорушень разом із виникненням інформаційних деліктів не виокремлюються, то суб'єктивні характеристики цих правопорушень, такі як види суб'єктів, деліктоздатність, вина та її форми, мета і мотиви, свідомо-вольовий характер будуть наповнені традиційним юридичним змістом, який не потребує додаткового розкриття. Натомість протиправність, небезпечність/шкідливість і об'єктивний вираз можуть мати свою інформаційну специфіку, чому приділимо увагу далі.

*Інформаційні делікти мають протиправний характер*, тобто вчиняються всупереч вимогам права. Основним об'єктом посягань таких правопорушень є інформаційні відносини регламентовані правовими нормами. При цьому особливості вияву протиправності інформаційного делікту наразі пояснюються залежно від галузі права, нормами якої передбачена відповідальність за такий делікт. Так, в межах адміністративного і кримінального права, з домінуючими імперативними нормами, протиправність інформаційних деліктів виявляється в порушенні безпосередніх заборон або у невиконанні обов'язків, встановлених законом. А, наприклад, у цивільному праві, для якого характерне диспозитивне регулювання та наявність договірної складової інституту юридичної відповідальності, інформаційні делікти полягатимуть у порушенні цивільних прав, невиконанні або неналежному виконанні цивільних обов'язків, що

можуть бути визначені як законом (актами цивільного законодавства), так і відповідним цивільно-правовим договором.

*Інформаційні делікти мають суспільно-небезпечний/шкідливий характер.* Усвідомлення суспільної небезпечності та/або шкідливості інформаційних деліктів потребує особливої виваженості. Традиційний для навчальної юридичної літератури, проте не безсумнівний, розподіл правопорушень на суспільно-небезпечні й шкідливі як підстава відокремлення злочинів від проступків не забезпечує повноти розкриття природних рис явища “інформаційний делікт”.

Новітні інформаційні правопорушення, на відміну від інших, частіше виникають не поодинокі, а характеризуються масовістю, нерідко лавиноподібністю поширення, що спричинено їх латентністю, легкістю повторення, універсальністю і доступністю знарядь вчинення, ускладненістю виявлення, фіксації і розкриття тощо. Суспільна небезпека окремого такого правопорушення може бути непомітною, але вона реальна і цілком очевидна, якщо інформаційні делікти певного виду розглядати в сукупності.

Окрім того, вітчизняна юридична наука має альтернативні концепти суспільної небезпечності правопорушень. Серед них найбільш поширеною є ідея “генетичного” зв’язку усіх видів правопорушень, завдяки чому певна міра суспільної небезпеки притаманна їм усім, а не тільки злочинам. Але і сьогодні деякі автори, зокрема О.М. Селезньова і В.В. Руданець, дискутуючи про сутність та ознаки правопорушень в інформаційній сфері, усе ж таки вдаються до їх формального розподілу на соціально-небезпечні й шкідливі [2, с. 143], з чим важко погодитися, зважаючи на попередні доводи.

Отже, наукова актуальність розгляду небезпечності/шкідливості інформаційних деліктів полягає не у здійсненні видової диференціації на злочини й проступки, а у відповідному вимогам часу науковому осмисленні обох цих характеристик як неоднорядкових. З огляду на це, неможливо не підтримати думки В.К. Колпакова, який, досліджуючи адміністративно-деліктний правовий феномен, зазначає, що в системі сучасних знань про адміністративний проступок конкурування концепцій суспільної небезпечності/шкідливості себе вичерпало. Суспільну небезпеку і суспільну шкоду в контексті дослідження ознак адміністративного проступку необхідно розглядати в діалектичному співвідношенні з урахуванням сучасних досягнень юридичних, філософських, соціологічних та інших наук [5, с. 165-187]. Очевидно, що наведені роздуми повною мірою стосуються не тільки адміністративних, а й інформаційних деліктів у цілому.

*Інформаційний делікт – це діяння.* Конкретний інформаційний делікт є актом поведінки в межах системи інформаційних відносин, сформованих суспільством і врегульованих правом.

Як специфічне діяння інформаційний делікт, характеризують, по-перше, певний «простір», утворений внаслідок інформатизації соціального життя, до якого належить об’єктивний прояв протиправної поведінки (реальна дія чи бездіяльність), по-друге, можливі варіації такого об’єктивного прояву з характерними для них унікальними рисами, зумовленими власне інформаційністю.

Необхідно відзначити, що загальноновживана назва “правопорушення в інформаційній сфері”, є лише абстрактним позначенням наявності певних зв’язків правопорушення з інформаційними явищами. У контексті ж конкретизації тієї реальності, в якій існує (вчиняється) інформаційний делікт, поняття “інформаційна сфера” виглядає дещо надмірним, адже зміст його доволі широкий і дискусійний та не обмежується правовим ракурсом. Існування поведінкових проявів інформаційного



делікту лежить скоріш у певному “сегменті”, утвореному сполученням інформаційної і правової сфер, або, що буде точніше, у сфері інформаційних правовідносин.

Для правової науки інформаційний делікт є передусім об’єктом правової дійсності, що осмислюється й перетворюється на відповідних методологічних засадах. З огляду на наукову міждисциплінарність, юридичну міжгалузевість, територіальну і юрисдикційну транскордонність явища “інформаційний делікт”, особливу цінність для його дослідження становить методологія просторового мислення, саме як складова правової методології.

Не вдаючись до дискусії щодо змісту та співвідношення загальних понять “сфера” та “простір”, необхідно зазначити, що особливість просторового підходу в юридичній науці пов’язана не тільки із своєрідністю юридичного розуміння поняття “простір” (зокрема, простору як форми соціального буття, для якого не обов’язкові прив’язки до фізичного простору та обмеження кордонами), а й своєрідністю та багатоманітністю права як соціального явища, особливостями його пізнання [6, с. 32-38].

Таким чином, інформаційні правопорушення – це протиправні діяння у сфері інформаційних правовідносин, але власні юридичні образи (моделі, концепції) як конкретні види інформаційних деліктів із відповідними правовими наслідками в формі юридичної відповідальності вони отримують у певному правовому просторі (національному, європейському, галузевому тощо) з притаманними йому ідеалами, цінностями, принципами, методами, зокрема привнесеними інформатизацією.

Юридично значущі ознаки інформаційного делікту, як і всіх інших правопорушень, узагальнюються в конструкції юридичного складу. Особливості видового розмаїття і нормативної фіксації складів інформаційних деліктів у правовому просторі певної держави будуть залежати від доктринальних тенденцій, правових традицій, юридичної техніки, форм писаного права тощо, притаманних національній правовій системі, а також вимог відповідних міжнародних актів.

Разом із тим, міжгалузевий характер юридичної відповідальності за інформаційні делікти, вимагає вивчення складів інформаційних деліктів з позицій тих галузей права, якими така відповідальність передбачена. Наприклад, спираючись на класифікації складів адміністративних правопорушень [5, с. 157-165], склади інформаційних деліктів також можна диференціювати за ступенем суспільної небезпеки (основні і кваліфіковані), за характером шкоди (матеріальні і формальні), за суб’єктом (особисті і службові), за структурою (однозначні й альтернативні), за особливостями конструкції (описові і бланкетні). А в цивільному праві склад інформаційних деліктів необхідно розглядати крізь призму своєрідної концепції складу цивільного правопорушення як сукупності загальних (типових) умов, наявність яких необхідна для покладення відповідальності на порушника цивільних прав та обов’язків, що може мати договірний і недоговірний характер.

Проте, в будь-якому разі, розглянута вище загальна інформаційна специфіка протиправності, суспільної небезпечності/шкідливості й об’єктивації інформаційного делікту як діяння позначається на сприйнятті елементів його юридичного складу, насамперед, об’єкта і об’єктивної сторони. Саме в цих елементах складу знаходять своє місце ті юридичні ознаки, які дають змогу виокремити інформаційний делікт серед інших правопорушень. Про відсутність певної домінантної інформаційності суб’єкта і суб’єктивної сторони інформаційного делікту свідчить і достатньо традиційний їх розгляд авторами профільних наукових публікацій [7 – 9].

*Об'єктом правопорушення* завжди є регламентовані правом суспільні відносини. Їх урегульованість, упорядкованість являє собою ту загальносоціальну і правову цінність, яка передусім “потерпає” від неправомірних діянь.

Якщо інформаційні делікти розглядати в максимально широкому розумінні і, відповідно, виділяти їх не тільки за об'єктом, а й за елементами об'єктивної сторони (шляхом, способом здійснення правопорушення) [1], то до об'єктів таких правопорушень належатимуть як інформаційні правовідносини, незалежно від способів посягання на них, так і інші правовідносини, що порушуються протиправними діями, які вчиняються з безпосереднім використанням інформаційних технологій, засобів, систем.

Проте іманентну інформаційну природу, яка являє собою первинний інтерес для науки інформаційного права, мають тільки інформаційні делікти у вузькому розумінні. Їхнім об'єктом є суто інформаційні відносини – суспільні відносини, що виникають в інформаційній сфері, в процесі або як наслідок інформаційної діяльності, та охороняються правом.

Серед інформаційних відносин об'єктне коло правопорушень складають: відносини в галузі масової інформації, авторського права, забезпечення інформаційної безпеки, бібліотечної та архівної справи; відносини у сфері встановленого правового режиму відкритої публічної інформації та інформації з обмеженим доступом, зокрема державної, комерційної, банківської, професійної таємниць, таємниці листування і телефонних розмов, службової інформації, персональних даних тощо.

До нематеріальних предметів правопорушень у сфері інформаційних відносин можна віднести відомості про осіб, предмети, факти, події, явища незалежно від форми їхнього подання, а також комп'ютерні дані; до матеріальних – носії інформації, засоби обробки, зберігання, передавання (поширення) інформації.

*Об'єктивну сторону інформаційних деліктів* становить зовнішня вираженість правопорушення в формі діяння, негативні наслідки та причиново-наслідковий зв'язок між ними, звичайно, з урахуванням інтерпретації цих елементів різними галузями права. Разом із обов'язковими інформаційність делікту може виявлятися і у факультативних елементах об'єктивної сторони, найчастіше як спосіб вчинення.

Своєрідність інформаційних деліктів може зумовлювати певну нестандартність усвідомлення їх об'єктивної сторони. Це, передусім, стосується протиправних діянь у “кібернетичному просторі”, тобто просторі, сформованому інформаційно-комунікаційними системами, в якому проходять процеси перетворення (створення, зберігання, обміну, обробки та знищення) інформації, представленої у вигляді електронних комп'ютерних даних. Їх об'єктивна сторона може не містити звичного зовнішнього виразу протиправної поведінки суб'єкта, з яким чітко зіставляються конкретні наслідки [10, с. 218]. Так, порушення процесів обробки інформації в комп'ютерних системах здійснене комп'ютерним вірусом (шкідливим програмним забезпеченням), який діє і поширюється некеровано та несвідомо переноситься користувачами, тільки на перший погляд, важко пов'язати з конкретно винною особою. Проте завжди є зловмисник, який створює і поширює такий вірус, або здійснює перше його впровадження в комп'ютерну систему чи мережу. У такому разі саме ініціювання шкідливих інформаційних процесів, управління ними необхідно вважати зовнішнім виразом протиправної поведінки деліквента.

Негативні наслідки інформаційних деліктів полягають передусім у завданні шкоди або створенні загрози інформаційним інтересам особи, суспільства, держави. Це фактично може виразитись як у конкретних матеріальних збитках так і в численних проявах загально відчутних нематеріальних втрат – підриві авторитету та ділової

репутації (окремих суб'єктів або держави в цілому), формуванні неадекватної (необґрунтованої) громадської думки та дезорієнтації населення, створенні суспільної паніки, дискредитації владних структур та їхніх рішень тощо.

Використання інформаційних технологій, систем, засобів як способів вчинення правопорушення виступає додатковою кваліфікуючою ознакою тільки тоді, коли законом визнана особлива небезпечність такого способу вчинення делікту (злочину), що відповідним чином зафіксовано в юридичному складі. Наприклад, ч. 3 ст. 190 ККУ “Шахрайство” передбачає посилене покарання за шахрайство, вчинене у великих розмірах, або шляхом незаконних операцій з використанням електронно-обчислювальної техніки. Тут, відповідно до кримінального закону, інформаційність правопорушення, навіть не будучи первинною ознакою, істотно впливає на суспільну небезпечність даного виду злочину і відповідальність за нього. Це є незайвим свідченням того, що подібні види деліктів (інформаційні за способом) певною мірою мають залишатися в фокусі інформаційної деліктології поряд із деліктами інформаційними за змістом.

### **Висновки.**

Сьогодні можна констатувати, що система знань про правопорушення в інформаційній сфері містить достатньо сформований комплекс ознак, на підставі яких інформаційний делікт розглядається як складна, специфічна, самостійна категорія правопорушень, яка зокрема має зіставлятися і з відповідним комплексним інститутом юридичної відповідальності.

Важливо, що інформаційність делікту може виявлятися не тільки в його об'єкті/предметі, а й в елементах об'єктивної сторони. Це зумовлює певну подвійність сприйняття інформаційних деліктів – як іманентно інформаційних, так і інших (зокрема традиційних деліктів) з набутою інформаційністю. Такий підхід загалом сприятиме адаптації механізмів юридичної відповідальності до всіх проявів інформаційності різних деліктів.

Інакше кажучи, базис ідеї “інформаційної” юридичної відповідальності мають скласти здобутки інформаційної деліктології, а подальша юридична обробка і прагматизація вже набутих знань повинні стати основою удосконалення комплексного інституту юридичної відповідальності в інформаційній сфері як фундаментального правового засобу, механізму, гаранту, покликаного забезпечувати регулятивну, захисну і охоронну дієвість інформаційного права, без чого не можливе існування й розвиток сучасного громадянського та інформаційного суспільства.

### **Використана література**

1. Правдюк С.М. Інформаційні правопорушення: автореф. дис. ...канд. юрид. наук: спец. 12.00.07 - адміністративне право і процес; фінансове право; інформаційне право. Київ, 2015. С. 8-9.
2. Селезньова О.М., Руданець В.В. Концепти розуміння сутності та ознак правопорушення в інформаційній сфері. *Право і суспільство*. 2017. № 3. Ч. 2. С. 144.
3. Тихомиров О.О. Інформаційні правопорушення: теоретико-правова концепція. *Інформаційна безпека людини, суспільства, держави*. 2015. № 1(17). С. 38-47.
4. Письменицький А.А. Формування концепту інформаційно-правової відповідальності в системі теорії юридичних санкцій: матер. VIII міжнар. наук.-практ. конф. *Актуальні проблеми методики навчання історії, правознавства та суспільствознавчих дисциплін*. Харків, 2016. № 8. С. 114-123.
5. Колпаков В.К. Адміністративно-деліктний правовий феномен: монографія. Київ: Юрінком Інтер, 2004. С. 165-187 с.

6. Тихомиров О.Д. Просторовий вимір права: проблеми методологічного осмислення. *Право України*. 2013. № 3-4. С. 32-38.

7. Настюк В.Я., Бєлевцева В.В. Загальноправова характеристика адміністративної відповідальності за інформаційні правопорушення. *Інформація і право*. № 1(7)/2013. С. 151-157.

8. Волкова А.О. Особливості юридичної відповідальності за правопорушення в інформаційній сфері. *Правова інформатика*. № 1(41)/2014. С. 72-80.

9. Коваленко Л.П. Деякі питання щодо правопорушень в інформаційній сфері. *Форум права*. 2013. № 4. С. 158-167.

10. Теорія держави і права: навч. посіб. для підгот. фахівців з інформ. безпеки / О.О. Тихомиров, М.М. Мікуліна, Ю.А. Іванов та ін.; за заг. ред. Л.М. Стрельбицької. Київ: Нац. акад. СБУ, 2016. 332 с.

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

УДК 35.078.3:007

КУШНІР І.П., кандидат юридичних наук, старший викладач кафедри теорії та історії держави і права та приватно-правових дисциплін
Національної академії Державної прикордонної служби України
імені Б. Хмельницького

АДМІНІСТРАТИВНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ІНФОРМАЦІЮ У ПРИКОРДОННІЙ СФЕРІ

Анотація. У статті досліджені адміністративні правопорушення законодавства про інформацію у прикордонній сфері. Визначені особливості відповідальності у даній сфері. Проаналізовані норми адміністративного законодавства та наукові праці дозволили окреслити проблеми правового регулювання даної сфери та визначити напрямки їх удосконалення.

Ключові слова: адміністративна відповідальність, правопорушення, інформація, Державна прикордонна служба України, прикордонна сфера.

Summary. The article investigates administrative violations of legislation on information in the border sphere. The peculiarities of responsibility in this area are defined. The analysed norms of administrative legislation and scientific works enabled to outline the problems of legal regulations of this sphere and determine the directions of their improvement.

Keywords: administrative responsibility, violation, information, the State Border Guard Service of Ukraine, border sphere.

Аннотация. В статье исследованы административные правонарушения законодательства об информации в пограничной сфере. Определены особенности ответственности в данной сфере. Проанализированные нормы административного законодательства и научные труды позволили очертить проблемы правового регулирования данной сферы и определить направления их совершенствования.

Ключевые слова: административная ответственность, правонарушение, информация, Государственная пограничная служба Украины, пограничная сфера.

Постановка проблеми. Питання збереження та захисту інформації як об'єкта інформаційних відносин сьогодні є досить важливими у всіх сферах державного та приватно-правового життя, особливо коли йде мова про діяльність органів публічної адміністрації, які є розпорядниками інформації у ввіреній їм державою й громадянами (як реалізація безпосередньої демократії) сфері правового регулювання. Державна прикордонна служба України (далі – ДПСУ) здійснює інформаційну діяльність в інтересах охорони державного кордону та реалізації права кожної людини, пов'язаного з вільним перетинанням державного кордону [1, с. 166]. Разом з розширенням меж інформаційної відкритості й інформаційної свободи у сучасному суспільстві актуалізуються питання дотримання інформаційних прав, їх збереження та захист усіх суб'єктів інформаційних відносин у прикордонній сфері. Охорона права на інформацію передбачена чинним законодавством [2, п. 1 ст. 7], у тому числі створена в процесі діяльності ДПСУ [2, п. 4 ст. 7]. Одним з дієвих засобів охорони інформаційних прав є застосування адміністративної відповідальності у разі їх порушення чи недотримання.

О.О. Тихомиров зазначає, що особливого значення набуває комплекс дієвих правових охоронних механізмів в інформаційній сфері, за умов низького рівня правосвідомості суспільства, якому сьогодні українські законодавці не приділяють

достатню увагу. Невирішеність означеної проблеми призводить до неповноти правового забезпечення і зниження ефективності правового впливу [3, с. 149].

Результати аналізу наукових публікацій. Питання адміністративної відповідальності висвітлені в наукових працях під різним кутом зору: як вид юридичної відповідальності в інформаційній сфері, порушення інформаційних прав, посягання на інформаційні відносини, забезпечення інформаційної безпеки, зокрема такими науковцями, як: І.В. Аристова, А.М. Благодарний, Л.П. Коваленко, В.А. Ліпкан, Ю.Є. Максименко, А.І. Марущак, В.В. Сидоренко, О.В. Стоєцький, О.О. Тихомиров, О.В. Чуприна та іншими. Норми інформаційного законодавства, як і відповідальність за їх порушення, не мають чіткої систематизації у зв'язку з комплексним характером цієї галузі й недосконалістю правотворчих процесів. Тому спробуємо синтезувати в даній статті нормативне закріплення та наукові підходи відносно висвітлення особливостей адміністративної відповідальності за порушення законодавства про інформацію у прикордонній сфері, якій до сьогодні у такому контексті не було приділено належної уваги.

Метою статті є аналіз адміністративної відповідальності за порушення законодавства про інформацію у прикордонній сфері, визначення її особливостей, проблемних аспектів та вироблення пропозицій щодо удосконалення.

Виклад основного матеріалу. Правове закріплення, урегулювання та розширення меж інформаційних відносин потребує правових механізмів захисту у разі посягання на відповідну інформацію, порушення (недотримання) інформаційних прав громадян чи ДПСУ. Однією з гарантій права на інформацію є встановлення відповідальності за порушення законодавства про інформацію [2, п. 1 ст. 6]. За встановленими законодавством підставами компетентні державні органи застосовують дисциплінарні, цивільно-правові, адміністративні або кримінальні засоби впливу [2, ст. 27]. Охоронні норми адміністративного права утворюють правовий фундамент протидії загрозам в інформаційній сфері [3, с. 148], а з урахуванням теми нашого дослідження і загрозам у прикордонній сфері. Ю.Є. Масименко наголошує, що тривалий час інформаційні правопорушення розглядалися крізь призму загроз інформаційній безпеці України, та зазначає, що сьогодні правопорушення в інформаційній сфері стосуються поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з баз даних, порушення технологій оброблення інформації, запуску програм-вірусів, троянів, фішингових програм, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо [4].

Л.П. Коваленко зазначає, що КУпАП передбачає адміністративну відповідальність за порушення права на окремі види інформації, відмову в наданні інформації, надання неповної або недостовірної інформації, втрату інформації [5, с. 162]. Обсяг і характер таких правопорушень постійно розширюється із розвитком інформаційного суспільства, інформаційних ресурсів та потребує своєчасного виявлення і застосування відповідальності за їх вчинення, зокрема й у прикордонній сфері.

Підставою для застосування адміністративно-деліктних норм і настання адміністративної відповідальності за невиконання інформаційного законодавства є вчинення інформаційного правопорушення. Суть зв'язку правопорушення з інформацією виявляється у його посяганні на певний порядок і правовідносини:

- щодо формування й використання інформаційних ресурсів на основі створення, збирання, оброблення, накопичення, зберігання, пошуку, поширення і надання інформації;
- створення і застосування інформаційних технологій та засобів їхнього забезпечення;
- захисту інформації та прав суб'єктів інформаційних відносин [6, с. 214].

Юридичною ознакою, що виділяє інформаційні правопорушення серед усіх інших, виступає присутність інформаційних компонентів у їхньому складі:

1) як об'єкта правопорушення – якщо протиправне діяння спрямоване проти інформаційних відносин, або як предмета правопорушення – якщо протиправне діяння спрямоване проти інформації та її носіїв, інформаційних засобів і систем;

2) як елемента об'єктивної сторони правопорушення, що вказує спосіб, шлях здійснення протиправного діяння – у разі його вчинення з використанням інформаційних технологій і засобів. Усі інші юридичні ознаки інформаційного правопорушення відповідають традиційній конструкції правопорушення в теорії права, проте можуть мати певні особливості, зумовлені інформаційною природою [6, с. 217].

Посилаючись на відсутність у чинному інформаційному законодавстві поняття інформаційного правопорушення, Л.П. Коваленко зробив акцент на об'єктах інформаційного правопорушення (одержання, використання, поширення та зберігання учасниками інформаційних правовідносин інформації) та сформулював дане поняття. Інформаційне правопорушення (проступок) – це протиправна, винна (умисна або необережна) дія чи бездіяльність, яка посягає на врегульовані законами суспільні відносини, які виникають та існують при здійсненні інформаційної діяльності, а саме: при одержанні, використанні, поширенні та зберіганні учасниками інформаційних правовідносин інформації і за яку законом передбачено інформаційну відповідальність [5, с. 158].

О.В. Стоєцький пропонує поділяти адміністративні правопорушення, що посягають на суспільні відносини у сфері: збирання інформації; зберігання інформації; використання інформації; поширення інформації [7, с. 10].

Такі підходи відображають посягання на окремі види інформаційної діяльності, закріплені в статті 9 Закону України “Про інформацію” (створення, збирання, одержання, зберігання, використання, поширення), а отже у такому випадку адміністративні правопорушення посягають на порядок інформаційної діяльності.

Інформаційне правопорушення характеризується тим, що завдає шкоди (небезпеки) інформаційним правам чи свободам людини та громадянина, інформаційній інфраструктурі держави чи вчиняється за допомогою інформаційно-телекомунікаційних технологій або засобів зв'язку [4]. Інформаційне правопорушення у прикордонній сфері, крім цього, завдає шкоди прикордонній безпеці та може вчинятись з використанням службового становища.

Ураховуючи особливості прикордонної сфери, у разі порушення законодавства про інформацію, наслідком якого є настання адміністративної відповідальності, варто зупинитись на характеристиці суб'єктного складу правопорушення. З цього приводу А.І. Марущак звертає увагу на те, що відповідальності підлягають як винні посадові особи (у необґрунтованій відмові в наданні інформації, порушенні встановленого терміну її представлення без поважних причин, безпідставній відмові від поширення певної інформації тощо), так і громадяни (які мають бажання і інтерес до отримання певної інформації і які у своєму бажанні можуть перейти межі дозволеної правомірної поведінки) [8, с. 456].

Відповідно до Кодексу України про адміністративні правопорушення (далі – КУпАП) суб'єктами адміністративного правопорушення є особи, які досягли на момент вчинення адміністративного правопорушення шістнадцятирічного віку [9, ст. 12], та посадові особи за недодержання установлених правил, забезпечення виконання яких входить до їх службових обов'язків [9, ст. 14]. Отже, для досліджуваного різновиду адміністративного правопорушення у прикордонній сфері характерним є як загальний, так і спеціальний суб'єкт.

Загальним суб'єктом досліджуваних правопорушень у прикордонній сфері може бути громадянин України, іноземний громадянин і особа без громадянства, на яких може розповсюджуватись адміністративна відповідальність за статтями 204-1 “Незаконне перетинання або спроба незаконного перетинання державного кордону України” та 204-4 “Порушення порядку в'їзду до району проведення антитерористичної операції або виїзду з нього” КУпАП, у частині перетинання або спроби перетинання державного кордону України в пунктах пропуску через державний кордон України (в контрольних пунктах в'їзду-виїзду) з використанням підробленого документа чи таких, що містять недостовірні відомості про особу.

Зважаючи на поняття “паспортний документ”, визначене Законом України “Про прикордонний контроль” [10, п. 12 ч. 1 ст. 1], який є підставою для перетинання державного кордону України [10, ч. 1 ст. 1], підроблений документ може містити неправдиву інформацію про особу, яка перетинає державний кордон, щодо її громадянства, підтвердження особи пред'явника, дійсного права на в'їзд або виїзд з держави. Отже, за подання неправдивої та недостовірної інформації про особу та з приводу наявної підстави перетинання державного кордону настає адміністративна відповідальність за статтями 204-1 та 204-4 КУпАП.

Спеціальними суб'єктами є посадові особи ДПСУ. Відповідно до статті 14 Закону України “Про Державну прикордонну службу України” особовий склад ДПСУ складається із військовослужбовців і працівників ДПСУ. Щодо працівників ДПСУ як суб'єктів адміністративної відповідальності, на них розповсюджуються загальні підстави відносно посадових осіб, що порушили законодавство про інформацію з урахуванням повноважень ДПСУ, за такі правопорушення:

- незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень (ст. 172-8 КУпАП);
- порушення законодавства у сфері захисту персональних даних (ст. 188-39 КУпАП);
- порушення законодавства про державну реєстрацію нормативно-правових актів (ст. 188-41 КУпАП);
- порушення законодавства про державну таємницю (ст. 212-2 КУпАП);
- порушення права на інформацію та права на звернення (ст. 212-3 КУпАП);
- порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію (ст. 212-5 КУпАП).

Суб'єктом інформаційного правопорушення згідно зі статтею 212-6 КУпАП (здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем) може бути будь-яка особа що посягає на встановлений порядок оброблення та зберігання інформації у базах даних ДПСУ, яка досягла віку адміністративної відповідальності. Тобто як загальний, так і спеціальний суб'єкт (посадові особи ДПСУ) підлягає адміністративній відповідальності в даному випадку.

З приводу військовослужбовців як суб'єктів адміністративної відповідальності існують особливості визначені у статті 15 КУпАП, згідно з якою військовослужбовці як посадові особи, що вчинили адміністративне правопорушення, несуть відповідальність за дисциплінарними статутами. Винятком щодо інформаційних правопорушень є порушення правил, норм і стандартів, що стосуються:

- вчинення правопорушень, пов'язаних з корупцією;
- здійснення незаконного зберігання спеціальних технічних засобів негласного отримання інформації;
- порушення законодавства про державну таємницю;
- порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію [9, ч. 1 ст. 15]. У цих випадках військовослужбовці ДПСУ несуть адміністративну відповідальність на загальних підставах за порушення законодавства про інформацію [9, ч. 1 ст. 15].

У такому разі виявляється певна неузгодженість положень статті 15 КУпАП та його доповнення у 2015 році главою 13-Б “Військові адміністративні правопорушення”. Зокрема, відносно теми нашого дослідження розглянемо статтю 172-16 “Бездіяльність військової влади” цієї глави. Дана стаття передбачає накладення штрафу або арешт з утриманням на гауптвахті, для військовослужбовців за “ненаправлення військовою службовою особою до органу досудового розслідування повідомлення про підлеглого, який вчинив кримінальне правопорушення”. Отже, згідно із статтею 15 КУпАП військовослужбовець у разі приховування інформації про підлеглого, який вчинив злочин, повинен нести дисциплінарну відповідальність, а згідно зі статтею 172-16, суб'єктом якого може бути лише військовослужбовець, – адміністративну. Очевидно, що коли Кодекс було доповнено главою 13-Б, законодавець залишив поза увагою момент узгодження її зі змістом норми статті 15.

Для військовослужбовців – посадових осіб ДПСУ за порушення інформаційного законодавства згідно зі статтею 15 може бути застосована адміністративна відповідальність за такими статтями КУпАП:

- 172-8 (незаконне використання інформації, що стала відома особі у зв'язку з виконанням службових або інших визначених законом повноважень);
- 195-5 (незаконне зберігання спеціальних технічних засобів негласного отримання інформації);
- 212-2 (порушення законодавства про державну таємницю);
- 212-5 (порушення порядку обліку, зберігання і використання документів та інших матеріальних носіїв інформації, що містять службову інформацію).

За вчинення інших інформаційних правопорушень, передбачених ст. 188-39, 188-41; 212-3, 212-6 КУпАП, військовослужбовці несуть дисциплінарну відповідальність.

Тому з урахуванням розвитку інформаційного суспільства, інформаційних відносин у прикордонній сфері та вимог часу вважаємо за необхідне внести зміни до статті 15 КУпАП в частині, що адміністративна відповідальність для військовослужбовців на загальних підставах, передбачених КУпАП, настає у разі вчинення правопорушень, передбачених главою 13-Б, та за порушення законодавства про інформацію. Вважаємо, що до військовослужбовців за вчинення окресленого у цій науковій статті різновиду адміністративних правопорушень повинні застосовуватись не дисциплінарні стягнення, а заходи адміністративної відповідальності.

Крім характерних для прикордонної сфери прогалин, у КУпАП існують і загальні проблемні питання, вирішення яких сприятиме підвищенню дієвості адміністративних

заходів впливу охоронного характеру для інформаційних відносин. З урахуванням аналізу змісту КУпАП варто наголосити на відсутності у ньому системності норм за порушення законодавства про інформацію, що значно ускладнює пошук інформації про склади адміністративних правопорушень даного виду, та застосування відповідальності.

В.А. Ліпкан та Ю.Є. Максименко, дослідивши основи формування інформаційної деліктології, роблять акцент на несистематизованості в окремому розділі та розпорошенні в різних розділах (главах) Кодексу України про адміністративні правопорушення адміністративних деліктів інформаційного характеру [11].

Крім цього, проблемність у цій сфері, зазначає О.В. Стоєцький, полягає у тому, що норми КУпАП, які встановлюють відповідальність у сфері інформаційної безпеки, дублюються нормами інших нормативно-правових актів, які, у свою чергу, інколи навіть прямо суперечать його нормам [7, с. 9].

Висновки.

Отже, адміністративній відповідальності за порушення законодавства про інформацію у прикордонній сфері характерні такі особливості:

- є різновидом адміністративної відповідальності, що передбачена за вчинення правопорушень, що містяться у різних розділах КУпАП та інших нормативно-правових актах, які врегульовують інформаційну діяльність та забезпечення права на інформацію (Закони України “Про інформацію”, “Про держану таємницю”, “Про захист персональних даних”, “Про доступ до публічної інформації”, “Про захист інформації в інформаційно-телекомунікаційних системах” тощо);
- адміністративній відповідальності підлягають особи, що перетинають державний кордон України; посадові особи ДПСУ (військовослужбовці та працівники); будь-яка особа у межах ст. 212-6 КУпАП;
- до військовослужбовців ДПСУ передбачено (ст. 15 КУпАП) застосування як дисциплінарних, так і адміністративних стягнень, що у деяких статтях КУпАП є неузгодженим і суперечним.

Окреслені проблемні питання адміністративної відповідальності за порушення законодавства про інформацію у прикордонній сфері та запропоновані напрямки удосконалення потребують подальшої розширеної конкретизації.

Використана література

1. Кушнір І.П. Інформаційно-правова діяльність Державної прикордонної служби України: нормативно-правовий аспект. *Конституційно-правові академічні студії*. 2018. № 2. С. 165-170.
2. Про інформацію: Закон України від 02.10.92 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650. URL: <http://zakon3.rada.gov.ua/laws/show/2657-12>
3. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави : монографія / за заг. ред. Р.А. Калюжного. Київ: Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. 196 с.
4. Максименко Ю. Є. Інформаційні правопорушення: поняття та ознаки. *Глобальна організація союзницького лідерства*. 2014. URL: <http://goal-int.org/informacijni-pravoporushennya-ponyattya-ta-oznaki/>.
5. Коваленко Л.П. Деякі питання щодо правопорушень в інформаційній сфері. *Форум права*. 2013. № 4. С. 158-167. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2013_4_29
6. Теорія держави і права : навч. посіб. для підгот. фахівців з інформ. безпеки / О.О. Тихомиров та ін.; за заг. ред. Л.М. Стрельбицької. Київ: Кондор, 2016. 332 с.
7. Стоєцький О.В. Адміністративна відповідальність за порушення у сфері інформаційної безпеки України: автореф. дис. ...канд. юрид. наук. Київ, 2013. 20 с.

8. Марущак А.І. Інформаційне право: доступ до інформації: навчальний посібник. Київ: КНТ, 2007. 532 с.

9. Кодекс України про адміністративні правопорушення: Закон України від 07.12.84 р. № 8073-X. URL: <https://zakon.rada.gov.ua/laws/show/80731-10>

10. Про прикордонний контроль: Закон України від 05.11.09 р. № 1710-VI. *Відомості Верховної Ради України*. 2010. № 6. С. 46.

11. Ліпкан В.А., Максименко Ю.Є. Засади розвитку інформаційної деліктології. *Право України*. 2013. № 10. С. 249-256. URL: <http://goal-int.org/zasadi-rozvitku-informacijnoi-deliktologii>

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

УДК 007:34.111

**КРАВЧУК І.М.**, здобувач наукового ступеня кандидата юридичних наук,  
НТУУ “КПІ ім. Ігоря Сікорського”

## **ПРАВОВІ ОСОБЛИВОСТІ ІНФОРМАЦІЙНИХ СУСПІЛЬНИХ ВІДНОСИН ПРИ НАДАННІ ДИСТАНЦІЙНИХ АДМІНІСТРАТИВНИХ ПОСЛУГ**

**Анотація.** Розглянуто правові особливості інформаційних відносин, що мають місце в процесі отримання адміністративних послуг, які надаються за допомогою Інтернет-технологій. На основі визначення та аналізу етапів процесу надання дистанційних адміністративних послуг висвітлено правові особливості інформаційних відносин між суб'єктами, а також з'ясовані перспективи подальших правових досліджень в цьому напрямку.

**Ключові слова:** інформаційні суспільні відносини, інформаційна взаємодія, адміністративні послуги, Інтернет-технології.

**Summary.** Author considers legal peculiarities of information relations that occur in the process of obtaining administrative services provided through Internet technologies. The analysis of process steps involved in providing remote administrative services highlights the relationships between entities entering into relations with information and clarifies the prospects for further research in this area.

**Keywords:** information public relations, information interaction, administrative services, Internet technology.

**Аннотация.** Рассмотрены правовые особенности информационных отношений, имеющие место в процессе получения административных услуг, предоставляемые с помощью интернет-технологий. На основе анализа этапов процесса предоставления дистанционных административных услуг изложены правовые особенности информационных отношений между субъектами, а также выяснены перспективы дальнейших исследований в этом направлении.

**Ключевые слова:** информационные общественные отношения, информационное взаимодействие, административные услуги, Интернет-технологии.

**Постановка проблеми.** Правовий інститут надання адміністративних послуг призначено для забезпечення прав та інтересів людини органами державної влади відповідно до їх повноважень, що визначено законом. Стан системи надання адміністративних послуг в державі безпосередньо характеризує відношення державних інституцій до пересічного громадянина та впливає на формування рівня довіри суспільства до влади. Тому в розвинутих демократичних країнах приділяється пильна увага щодо формування правових умов надання адміністративних послуг, зокрема, в дистанційному режимі, що створює міцне підґрунтя для усунення багатьох недоліків, які, як правило, мають місце при наданні таких послуг без застосування Інтернет-технологій. Багато дослідників вважає, що однією з основних причин розчарування населення нашої країни в системі надання адміністративних послуг є вкрай незадовільний стан інформаційної взаємодії їх надавачів та отримувачів [1; 2]. Тому вдосконалення правового регулювання інформаційних суспільних відносин, які супроводжують процес надання адміністративних послуг, дозволить забезпечити зручність, швидкість, якість, доступність, безвідмовність з бюрократичних причин при наданні таких послуг. У зв'язку з цим особливої актуальності набуває питання визначення правових особливостей інформаційних суспільних відносин, що виникають між державою і громадянами на окремих етапах інформаційної взаємодії в системі надання дистанційних адміністративних послуг.

**Результати аналізу наукових публікацій.** Проблеми правового регулювання надання адміністративних послуг досліджували в своїх роботах Ю.М. Жук [1], К.С. Кучма [12], М.О. Репецька [2], Д.В. Сущенко [6], В.П. Тимошук [3], І.О. Тищенко [7], К.А. Фуглевич [13] та ін. В частині правового регулювання інформаційних відносин проводили наукові розробки І.В. Арістова [4], К.І. Беляков [10], О.А. Баранов [11], В.В. Белєвцева [5] та багато ін. Проте, в науковій літературі недостатньо опрацьовані питання вдосконалення правового регулювання інформаційних суспільних відносин, які мають місце на кожному окремому етапі надання адміністративних послуг. Більш того, практично не досліджені такі суспільні відносини з урахуванням специфіки, що притаманна процесу надання адміністративних послуг з використанням Інтернет-технологій.

**Метою статті** є визначення правових особливостей суспільних відносин, що виникають в процесі інформаційної взаємодії на кожному окремому етапі між органами державної влади та місцевого самоврядування і громадянами при наданні дистанційних адміністративних послуг.

**Виклад основних положень.** Процес надання адміністративних послуг складається з певної послідовності дій, що зазначені у різних нормативно-правових актах [6] та спрямовані на досягнення певного результату, який здійснюється з метою сприяння реалізації та захисту прав, свобод та законних інтересів фізичних та юридичних осіб.

Тищенко І.О. в своїй роботі [7] звертає увагу на те, що послідовність дій при наданні адміністративних послуг як традиційним, так і дистанційним способом, незважаючи на їх конкретний тип, має певну логіку адміністративно-процедурної діяльності. Ця послідовність складається з відповідних етапів, які є самостійними частинами процесу надання послуг та різняться один від одного завданнями, інформаційними взаємозв'язками між суб'єктами тощо. Можна погодитись з позицією даного автора про те, що особливостями процесу надання дистанційних адміністративних послуг є те, що звернення за їх отриманням відбувається за допомогою Інтернет-технологій, а результат може бути надано як в паперовій, так і в електронній формі. Крім того, до подібних особливостей слід віднести і те, що процес надання супутніх документів, надання інформації про умови отримання послуги, а також перевірка статусу виконання дистанційної адміністративної послуги, може більш ефективно відбуватись за допомогою мережі Інтернет.

Аналізуючи особливості нормативного регулювання, що визначені в Законі України “Про адміністративні послуги” [8] та в постанові Кабінету Міністрів України “Про затвердження вимог до підготовки технологічної картки адміністративної послуги” [9], необхідно відзначити, що процес надання адміністративної послуги складається з наступних етапів:

- 1) подання заяви на отримання адміністративної послуги;
- 2) подання документів, довідок тощо для отримання адміністративної послуги;
- 3) опрацювання наданих заяв та документів суб'єктом надання адміністративної послуги;
- 4) прийняття рішення щодо можливості надання або відмови у наданні адміністративної послуги;
- 5) отримання результату надання адміністративної послуги.

Отже, розглянемо більш детально етапи процесу отримання адміністративних послуг, які надаються за допомогою Інтернет-технологій.

*Перший етап* – етап подачі заяви щодо надання адміністративної послуги. Допускається, що заява подається в письмовій, усній чи електронній формі. Але

письмова заява, яка подається особисто суб'єктом отримання послуги, може бути надіслана поштою або у випадках надання заяви в електронній формі, за допомогою засобів телекомунікацій. Перед етапом подання заяви може бути попередній етап – це етап консультування щодо умов надання конкретної адміністративної послуги, отримання бланку заяви та її заповнення.

*Другий етап* лише умовно можна виділити в окремий, так як він нерозривно пов'язаний з етапом подання заяви і включає в себе надання додаткових документів, довідок, виписок, квитанцій про оплату у випадку платної адміністративної послуги тощо. В Законі [8] встановлено, що для отримання адміністративної послуги суб'єкт звернення повинен надати документи, що містять інформацію про особу, у випадку відсутності цих відомостей у відповідних інформаційних базах в обсязі, достатньому для надання такої послуги.

*Третій етап* надання адміністративної послуги включає в себе опрацювання наданих заяв та супутніх документів суб'єктом надання адміністративної послуги. До таких дій з опрацювання слід віднести: отримання пакету документів, його реєстрацію, дослідження та оцінка матеріалів на відповідність інформаційної картки [8] певної адміністративної послуги. Цей етап має низку послідовних дій різних виконавців, що мають бути прописані в технологічній картці надання конкретної адміністративної послуги. Крім того, в технологічній картці адміністративної послуги зазначаються відповідальні посадові особи, структурні підрозділи, відповідальні за дії і рішення, а також чітко визначені строки їх виконання.

*Четвертий етап* – етап приймання рішення щодо надання відповіді по суті звернення. На цьому етапі відбуваються дії щодо юридичної оцінки відомостей, які надані суб'єктом отримання адміністративної послуги, узгодження результату зі структурними підрозділами і посадовими особами суб'єкта надання адміністративної послуги. Важливим моментом на цьому етапі є функціонування взаємодії між всіма структурними підрозділами та іншими відомствами, що беруть участь в наданні інформації, яка є необхідною для надання конкретної адміністративної послуги [9].

*На п'ятому етапі* процесу надання адміністративних послуг відбувається взаємодія щодо отримання відповіді (результату) здійснення владних повноважень суб'єктом надання адміністративних послуг за заявою фізичної або юридичної особи, спрямованих на набуття, зміну чи припинення прав та/або обов'язків такої особи.

Сукупність етапів надання адміністративних послуг утворюють єдиний ланцюжок дій з відповідними взаємозв'язками між суб'єктами отримання і надання адміністративних послуг (Мал. 1.).

Аналіз етапів процесу надання адміністративних послуг дозволяє зробити висновок про те, що весь процес від подання заяви до отримання адміністративного акту пов'язаний з оборотом інформації між суб'єктами надання та отримання адміністративних послуг. В такому випадку, вони вступають між собою в інформаційно-правові відносини [10; 11] і утворюють інформаційні взаємозв'язки, що показано на Мал. 2.

Так як процес надання адміністративної послуги має індивідуальний характер, то для початку інформаційної взаємодії щодо кожної конкретної послуги необхідно пройти етап отримання інформації: про саму адміністративну послугу, про суб'єкта звернення, який наділений повноваженнями щодо надання цієї конкретної послуги, про порядок отримання такої послуги, а також про перелік супутніх документів, які необхідно надати разом з заявою. Для кожної окремої послуги повинна складатись інформаційна картка, що містить відомості про певну адміністративну послугу. Як правило така

інформація розміщується на офіційному веб-сайті органу влади або на Єдиному державному порталі адміністративних послуг.



Мал. 1. Блок-схема процесу надання адміністративної послуги

Проте, сама інформаційна взаємодія починається з моменту передачі інформації у формі заяви. Так як законодавством реквізити такої заяви не визначені [12], то, доцільно віднести до складу інформації в заяві такі дані, як: назва адміністративної послуги, інформація про суб'єкта звернення (ПІБ заявника, місце проживання фізичної особи або місцезнаходження юридичної особи, дата і підпис). Необхідно звернути увагу на те, що перед заповненням бланку заяви, суб'єкт звернення повинен отримати повну інформацію щодо можливих варіантів ідентифікації особистості. Це не відноситься до початку процесу надання певної адміністративної послуги, але має значення для нашого предмету дослідження, так як, у випадку надання послуги в електронній формі, існують певні проблеми з отриманням бланку заяви та його заповненням безпосередньо на веб-сайті тому, що законодавчо не визначені вимоги щодо здійснення такої процедури.

Наступний етап є нерозривним з першим, так як до інформації про послугу і дані заявника, необхідно додати інформацію у вигляді вхідного пакету документів, які визначені для кожної конкретної адміністративної послуги. Наприклад, для переоформлення ліцензій на здійснення діяльності у сфері телекомунікацій необхідно

надати наступну інформацію у вигляді таких документів: ліцензія на здійснення діяльності у сфері телекомунікацій, що підлягає переоформленню, документи, які підтверджують зазначені зміни або їх нотаріально засвідчені копії.



Мал. 2. Загальна схема інформаційної взаємодії між суб'єктами надання та отримання адміністративної послуги

Оскільки існують адміністративні послуги, які потребують плати за її надання, то, у такому випадку, слід додати інформацію про оплату послуги у вигляді копії квитанції. Проте, проблемним питанням залишається визначення конкретних правових вимог



щодо подання оригіналів та/або копій документів у випадку використання при цьому Інтернет-технологій.

Після цього інформація, яка надійшла до суб'єкта надання адміністративної послуги, повинна бути зафіксована, оброблена і перевірена на достатність для порушення адміністративної справи [13].

До інформаційної взаємодії між суб'єктами надання та отримання адміністративних послуг на цьому етапі слід також віднести:

- надання та отримання інформації щодо реєстрації/відмови в реєстрації вхідного пакету документів;

- надання та отримання інформації щодо достатності/недостатності поданих документів для отримання адміністративної послуги;

- інформування про необхідність додаткового надання документів. Слід зауважити, що рівень правового регулювання процесу проходження етапів реєстрації, відмови та інформування про це в умовах використання засобів телекомунікацій є не достатнім.

На етапі винесення рішення відбувається логічне завершення третього етапу, який характеризується такими елементами інформаційної взаємодії, як інформування про хід розгляду звернення щодо отримання адміністративної послуги та про результати розгляду звернення щодо отримання адміністративної послуги (надання адміністративної послуги або відмова).

Наступний етап включає в себе інформаційну взаємодію щодо надання результату та його реєстрацію, а саме: процес інформування про можливість та умови отримання юридичного документу. На цьому етапі виникають труднощі з передачею результату в електронній формі.

Узагальнюючи питання інформаційної взаємодії, слід відзначити, що на всіх етапах процесу надання адміністративної послуги існує процес передачі інформації між суб'єктами звернення/отримання і суб'єктами надання такої послуги. Інформація, яка викладається в паперовому або електронному документах, повинна бути ідентичною. Разом з тим, у випадку використання електронного документу при наданні адміністративних послуг, існує відмінність у порядку визначення автентичності та місця подання інформації, що обумовлено особливостями застосування Інтернет-технологій. Тому правове регулювання отримання і надання інформації в електронній формі має ряд особливостей.

У випадку використання технологій “он-лайн” бажано втілювати в системі надання адміністративних послуг такий принцип, як інтерактивність, що дозволяє підтримувати інформаційний зв'язок між суб'єктами в режимі реального часу без будь-яких допоміжних засобів. Перед початком здійснення дій, суб'єкт отримання адміністративної послуги звертається он-лайн до суб'єкта надання такої послуги з метою отримання детальної інформації щодо надання послуги. До такої інформації слід віднести: строк надання послуги, необхідні додаткові документи, адміністративний збір, результат і способи його отримання, підстави для відмови, порядку оскарження рішень, нормативно-правові акти, якими керуються при наданні конкретної адміністративної послуги. У випадку надання такої інформації он-лайн, суб'єкт, що звертається за такою послугою повинен бути впевнений, що інформація офіційна, достовірна та повна. На сьогодні в Україні правовою основою для цього є Закон України “Про доступ до публічної інформації” [14], проте він не є достатнім для вирішення питань стосовно надання інформації щодо адміністративних послуг за умови використання Інтернет-технологій.

Подальше надання інформації з метою вираження волевиявлення для дистанційного отримання адміністративної послуги відбувається у вигляді заповнення електронної форми заяви. Законом [9] визначено, що суб'єкт надання адміністративних послуг забезпечує можливість безоплатного одержання суб'єктами звернення у достатній кількості бланків заяв та інших документів, необхідних для звернення щодо надання адміністративної послуги, в тому числі одержання бланків з веб-сайтів суб'єктів надання адміністративних послуг. Більш того, ця процедура може відбуватися за рахунок завантаження форми заяви з подальшим її поданням за допомогою електронної пошти. В таких випадках, для завантаження форми бланку вимагається авторизація автора на веб-сайті, який надає таку послугу. Як правило, авторизація суб'єкта отримання адміністративної послуги відбувається за рахунок використання електронного цифрового підпису. В режимі інтерактивності технічно є можливість занесення інформації в форму заяви методом заповнення безпосередньо на веб-сторінках, але, на сьогодні, механізм ідентифікації автора не врегульовано законодавством України.

На етапі надання супутніх документів суб'єкту звернення необхідно здійснити завантаження необхідних документів в електронній формі та прикріпити їх до заяви. Законом [8] встановлено, що суб'єкт надання адміністративної послуги не має права вимагати від суб'єкта звернення документи або інформацію для надання адміністративної послуги, що не передбачені законом.

На етапі обробки інформації та на етапі прийняття рішення щодо надання адміністративної послуги суб'єкт надання адміністративної послуги повинен здійснювати інформаційну взаємодію з суб'єктом отримання цієї послуги, а саме надавати інформацію щодо реєстрації заяви або вмотивованої відмови, інформувати про хід справи. Зворотній зв'язок може відбуватися шляхом надання інформаційних повідомлень в Персональному кабінеті суб'єкта звернення.

У випадках, коли необхідно отримати додаткові документи, що знаходяться у володінні інших органів влади, суб'єкт надання адміністративної послуги здійснює запит без участі суб'єкта звернення шляхом доступу до інформаційних систем чи баз даних інших суб'єктів надання адміністративних послуг, або через систему електронної взаємодії державних електронних інформаційних ресурсів. Правове регулювання електронної міжвідомчої взаємодії досить суперечливе та розташоване в різних нормативно-правових актах і не створює правових основ, які б забезпечували ефективне функціонування цього напрямку [2].

На етапі передачі результату адміністративної послуги відбувається інформаційна взаємодія між суб'єктами, яка характеризується можливістю отримання інформації як традиційним способом, так і за допомогою засобів телекомунікацій. Крім вище згаданих проблем правового регулювання інформаційних процесів, які притаманні попереднім етапам, на цьому етапі також потрібно вдосконалювати правову регламентацію передачі результату надання адміністративної послуги за допомогою Інтернет-технологій.

Необхідно зауважити, що результатом здійснення владних повноважень суб'єктом надання адміністративних послуг може бути паперовий або електронний документ. У випадку отримання електронного документу може виникнути необхідність його подальшого подання в деякі інші інстанції в паперовій формі. В Законі [8] зазначено, що електронний документ, у визначених законодавством випадках, може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії. Разом з тим, є ряд документів, які є результатом адміністративної послуги, але не можуть мати оригінал в електронній формі. Наприклад, при наданні послуг видачі паспорту громадянина України, суб'єкт звернення повинен отримати документ в паперовій формі, а інформацію щодо

місця, дати і часу отримання результату суб'єкт надання такої послуги може отримати шляхом надсилання інформаційного повідомлення в електронній формі до Персонального кабінету суб'єкта звернення. Для забезпечення належної організації надання інформації щодо результату процесу надання адміністративної послуги в найкоротший термін за умови використання засобів телекомунікацій необхідно встановити чіткі правові умови такої взаємодії.

### **Висновки.**

Визначення етапів процесу надання та отримання адміністративної послуги та аналіз їх особливостей дозволили класифікувати елементи інформаційної взаємодії суб'єктів, які вступають в інформаційні суспільні відносини, що, в свою чергу, дозволило виявити низку правових проблем, вирішення яких має значення для вдосконалення процесу надання адміністративних послуг, а саме:

- необхідність створення правових механізмів, що забезпечують отримання юридично значимої інформації про порядок надання дистанційних адміністративних послуг, заповнення екранних форм за умови юридичного підтвердженні волевиявлення суб'єкта отримання такої послуги;
- необхідність створення правових механізмів щодо забезпечення ідентифікації суб'єкта отримання адміністративної послуги в зручному для нього вигляді, а також забезпечення визначення місця проживання суб'єктів звернення;
- формування нормативно-правової бази щодо забезпечення регламентації міжвідомчої інформаційної взаємодії та інформаційної взаємодії між владою і громадянами на всіх етапах процесу надання дистанційних адміністративних послуг.
- удосконалення правових механізмів надання для паперових документів копії в електронній формі і навпаки.

**Перспективи подальших досліджень.** Вважаємо, що доречним буде проведення дослідження щодо об'єкту, змісту та суб'єктивного складу інформаційних правовідносин, які мають місце в процесі інформаційної взаємодії у сфері надання дистанційних адміністративних послуг.

### **Використана література**

1. Жук Ю.М. Надання адміністративних послуг населенню: орієнтація на якість. *Теорія та практика державного управління*. 2017. № 1(56). С. 137-145.
2. Репецька М.О. Організаційно-правові аспекти функціонування системи електронних адміністративних послуг в Україні. *Вісник Національного університету "Львівська політехніка"*. 2016. № 850. С. 99-106.
3. Тимошук В.П. Адміністративні послуги. Київ: ТОВ "Софія-А", 2012. 104 с.
4. Арістова І.В. Реалізація інформаційно-правового статусу органів виконавчої влади України в інформаційних правовідносинах. Київ: Видавничий центр НУБіП України, 2015. 250 с.
5. Белєвцева В.В. Теоретико-правові підходи до визначення поняття "інформація" через інформаційні правовідносини. *Інформація і право*. № 3(15)/2015. С. 5-10.
6. Сущенко Д.В. Общая характеристика понятия и признаков административных процедур в Украине. *Leges si viata*. 2018. № 9/2. С. 155-158.
7. Тищенко І.О. Адміністративні процедури надання електронних послуг публічною адміністрацією в Україні. *Форум права*. 2017. № 2. С. 124-129. URL: [http://nbuv.gov.ua/UJRN/FP\\_index.htm\\_2017\\_2\\_21](http://nbuv.gov.ua/UJRN/FP_index.htm_2017_2_21) (дата звернення: 18.02.2019).
8. Про адміністративні послуги: Закон України від 6.09.12 р. № 5203-VI (База даних "Законодавство України" / ВР України). URL: <https://zakon.rada.gov.ua/laws/show/5203-17> (дата звернення: 19.02.2019).

9. Про затвердження вимог до підготовки технологічної картки адміністративної послуги: Постанова Кабінету Міністрів України від 30.01.13 р. № 44 (База даних “Законодавство України” / ВР України). URL: <https://zakon.rada.gov.ua/laws/show/44-2013-%D0%BF> (дата звернення: 19.02.2019).

10. Беляков К.І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: “віртуальні правовідносини”. *Lex Portus*. 2016. № 2. С. 47-63. URL: <https://lexportus.net.ua/vipusk-2-2016/belyakov.pdf> (дата звернення: 20.02.2019).

11. Баранов О.А. Напрями перспективних досліджень у галузі інформаційного права. *Інформація і право*. № 2(17)/2016. С. 15-31.

12. Кучма К.С. Стадії провадження надання адміністративних послуг у сфері екології та природних ресурсів в Україні. *Науковий вісник Міжнародного гуманітарного університету*. 2016. №. 20. С. 73-76. URL: <http://vestnik-pravo.mgu.od.ua/archive/juspradenc20/21.pdf> (дата звернення: 21.02.2019).

13. Фуглевич К.А. Процедура предоставления административных услуг. *Legea si viata*. 2014. № 3/3. С. 191-195.

14. Про доступ до публічної інформації: Закон України від 13.01.11 р. № 2939-VI (База даних “Законодавство України” / ВР України). URL: <https://zakon4.rada.gov.ua/rada/show /2939-17> (дата звернення: 21.02.2019).

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

УДК 34:004

БЕЖЕВЕЦЬ А.М., аспірантка НТУУ “КПІ ім. Ігоря Сікорського”

ПРАВОВИЙ СТАТУС РОБОТІВ: ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ВИЗНАЧЕННЯ

Анотація. У статті проаналізовано сучасні наукові ідеї та концепції визначення правового статусу роботів зі штучним інтелектом. Розглянуто питання можливості визнання роботів суб'єктами відносин та визначення їх правосуб'єктності.

Ключові слова: робот, штучний інтелект, робототехніка, правовий статус робота, правосуб'єктність робота, електронна особа.

Summary. The article analyzes modern scientific ideas and concepts for determining the legal status of robots with artificial intelligence. The author investigated the issue of determination of legal personality of robots.

Keywords: robot, artificial intelligence, robotics, legal status of the robot, legal personality of the robot, electronic person.

Аннотация. В статье проанализированы современные научные идеи и концепции определения правового статуса роботов с искусственным интеллектом. Рассмотрен вопрос возможности признания роботов субъектами отношений и определения их правосубъектности.

Ключевые слова: робот, искусственный интеллект, робототехника, правовой статус робота, правосубъектность робота, электронное лицо.

Постановка проблеми. Сучасна тенденція глобальної цифровізації практично всіх сфер діяльності суспільства, що здійснює дуже суттєвий вплив на спрямованість та характер суспільних відносин, вимагає необхідності законодавчого реагування для формування адекватної правової бази з метою здійснення належного правового регулювання цих суспільних відносин.

Новітні технології, зокрема технології штучного інтелекту та Інтернету речей, Хмарних технологій, блокчейну, криптовалюти тощо, враховуючи темпи та спрямованість їх розвитку, не можуть і надалі залишатися поза увагою законодавчого регулювання, внаслідок їх впливу на трансформацію існуючих та формування нових суспільних відносин. На даному етапі деякі із зазначених відносин лише формуються, але в подальшому, можливо вже через 5 – 10 років, вони трансформуються в повноцінні правові інститути.

Впровадження роботів в повсякденне життя людей потребує цілеспрямованого впливу держави на ці трансформаційні та формуючі процеси суспільних відносин за допомогою спеціальних юридичних засобів і методів, які спрямовані на їх стабілізацію і упорядкування.

Навіть якщо роботи ще не стали звичайним явищем, то саме зараз, на етапі впровадження робототехніки і елементів штучного інтелекту існує реальна необхідність нормативно-правового визначення статусу роботів із повноцінним штучним інтелектом або відповідними його елементами – у залежності від спрямованості та характеру завдань, для вирішення яких вони створювалися.

Сьогодні ряд держав світу активно працює над проблемою необхідності врегулювання статусу та використання “кінцевих” продуктів технологій штучного інтелекту та робототехніки.

Сучасне вітчизняне законодавство, на жаль, не готове до настільки активного впровадження технологій і систем штучного інтелекту в життя людини, в економіку, в юридичну практику. А що стосується правосуб'єктності робототехніки зі штучним інтелектом, зараз тільки починається ця дискусія в науковій літературі.

Результати аналізу наукових публікацій. Правові аспекти визначення статусу робототехніки та штучного інтелекту є предметом дослідження науковців О.А. Баранова, Т.Г. Каткової, М.В. Карчевського, К.О. Хернес, С.Ю. Петряєва, О.Е. Радутного, Ю.М. Сидорчук, А. Сулина, Є.О. Харитонова, О.І. Харитонові, В.М. Фурашева, О.А. Ястребова та інших.

Метою статті є визначення сучасного стану правового регулювання суспільних відносин щодо статусу роботів зі штучним інтелектом та перспектив подальшого удосконалення законодавства у цій сфері.

Виклад основних положень. Як відомо, базисом існування будь-якого суспільства, в тому числі і людства в цілому, була, є і буде економіка. Цифровізація реального сектору економіки є головною складовою цифрової економіки та визначальним чинником зростання економіки в цілому, зокрема і самої цифрової індустрії, як виробника технологій. Цифрові технології в багатьох секторах є основою продуктових та виробничих стратегій. Їх перетворювальна сила змінює традиційні моделі бізнесу, виробничі ланцюги та процеси, зумовлює появу нових продуктів та послуг, платформ та інновацій [1].

Концепція розвитку цифрової економіки та суспільства України на 2018 – 2020 роки, схвалена розпорядженням Кабінету Міністрів України від 17 січня 2018 року № 67-р визначає необхідність створення оновленої концепції “розумного виробництва”, що ототожнюється з “четвертою промисловою революцією” та появою кіберфізичних систем. Індустрія 4.0 – наступний етап цифровізації виробництв та промисловості, на якому головну роль відіграють такі технології та концепти, як “Інтернет речей” (Internet of Things, IoT), “Великі дані” (Big Data), “Хмарні обчислення”, предиктивна аналітика, машинне навчання, машинна взаємодія, штучний інтелект, робототехніка, 3D-друк, доповнена реальність [1].

Однак, аналіз сучасного законодавства України свідчить, що вітчизняний законодавець приділяє поки що лише декларативну або, у кращому разі, дотичну увагу досліджуваному автором питанню.

Набагато більше уваги питанню правового регулювання суспільних відносин, які вже зазнали визначених змін або починають формуватися під час впровадження та використання робототехніки, в тому числі із застосуванням елементів штучного інтелекту, приділено в законодавстві таких країн як США, Німеччина, Японія тощо.

Урядом Японії ще у 2015 році затверджено Нову стратегію роботів (New Robot Strategy) [2]. Зазначеним документом сформовано концептуальні підходи до впровадження робототехніки на найближчі 5 років. Зокрема, Стратегією визначено, що роботи можуть використовуватись у всіх сферах повсякденного життя, в тому числі, наприклад, для допомоги літнім людям, для забезпечення безпеки і комфорту суспільства.

Наступним етапом розвитку робототехніки визначена тенденція Інтернету речей, коли роботи стають взаємопов'язаними для взаємного співробітництва як “мережевий” інструмент, що виходить за рамки окремих завдань у вигляді одного робота, за допомогою якого роботи будуть функціонувати не тільки як один робот, але і як частина різних систем.

В грудні 2017 року в конгрес США був внесений проект закону, який закріплює визначення поняття штучного інтелекту в законодавстві США.

У червні 2017 року в Німеччині було затверджено збірку етичних норм для роботизованих транспортних засобів (звіт Комісії з етики Федерального міністерства транспорту і цифрової інфраструктури Німеччини “Автоматизоване та під’єднане керування”) [3].

До перших кроків глобального законодавчого врегулювання питання правового статусу роботів зі штучним інтелектом або його елементами можна віднести Резолюцію, що у 2017 році розглянута Комітетом Європейського Парламенту з правових питань, яка містить пропозицію включити в законодавство ЄС поняття “розумний робот”, розробити систему реєстрації таких роботів, а також визначити правовий статус роботів як електронної особистості (електронної особи) [4].

Зазначений документ був неоднозначно сприйнятий суспільством, існують як адепти такої концепції, так і ті, хто категорично заперечує такі перспективи. Однак, безумовно, його можна вважати значним проривом, а може навіть і переворотом в суспільному усвідомленні місця та статусу робота на сучасному етапі розвитку людства.

Одночасно відбувається інтенсивне напрацювання методологічних і концептуальних підходів до вирішення питання про те, яким чином має здійснюватися правове регулювання розробки та застосування технологій штучного інтелекту та робототехніки.

Існує велика кількість дефініцій і пояснень термінів “робот”, “робототехніка”, “штучний інтелект”. Однак відсутнє єдине визначення зазначених термінів, оскільки жодне із запропонованих науковцями визначень не отримало схвалення більшості внаслідок відсутності консенсусу в світовому науковому товаристві. У зв’язку з чим можна відзначити, що формування єдиного визначення вказаних термінів в юридичній науці та законодавстві є проблемним питанням сьогодення.

Однак, на думку автора, відсутність на сьогодні єдиної, з наукової або законодавчої точок зору, дефініції хоча й ускладнює, проте не перешкоджає дослідженню питання про статус робота з елементами штучного інтелекту в системі правовідносин та аналізу сучасного національного законодавства й наукової думки з цією метою.

Досліджуючи вказану проблематику, автор статті виходить з необхідності визначити, чи є робот лише об’єктом правовідносин та чи може, у майбутньому, виступати суб’єктом правовідносин.

Проаналізувавши дослідження українських та зарубіжних науковців, які присвячені проблемі правового статусу, а саме, визначення правосуб’єктності роботів зі штучним інтелектом, підставно дійти висновку, що їх роль, місце та статус має регулюватися нормами цивільного законодавства у сукупності з нормами інформаційного права.

Учасниками цивільних відносин стаття 2 Цивільного кодексу України (далі – ЦК України) визначає фізичних осіб та юридичних осіб, а також державу Україна, Автономну Республіку Крим, територіальні громади, іноземні держави та інших суб’єктів публічного права.

Оскільки ця норма містить вичерпний перелік суб’єктів цивільних відносин, то можемо дійти висновку, що робот, навіть зі штучним інтелектом, не є суб’єктом суспільних відносин, а, відповідно, й суб’єктом правовідносин.

Враховуючи, що в статті 177 ЦК України визначено види об’єктів цивільних прав, та оскільки такий перелік не є вичерпним та підлягає розширеному тлумаченню, відповідно приходимо до висновку, що на сьогодні правовий статус роботів регулюється положеннями щодо об’єктів цивільних прав.

При цьому не можна погодитися із думкою А. Сулина, який вважає, що роль робота фактично може бути прирівняна до майна. Перелік об’єктів цивільних прав поповниться ще одним найменуванням, та цим проблема здебільшого буде вичерпана [5].

Цивільний кодекс України та інші акти цивільного законодавства України не містять поняття “робот”, “штучний інтелект”, у зв’язку з чим для подальшого визначення та конкретизації правового статусу робота як об’єкта правовідносин, необхідно застосовувати за аналогією норми, які стосуються об’єктів цивільних прав, виходячи із дефініцій “робота”, “штучний інтелект”, які містяться в науковій літературі.

Зокрема, на нашу думку, статусу робота найбільш відповідає положення статті 1187 ЦК України, де визначено, що джерелом підвищеної небезпеки є діяльність, пов’язана з використанням, зберіганням або утриманням транспортних засобів, механізмів та обладнання, використанням, зберіганням хімічних, радіоактивних, вибухо- і вогнебезпечних та інших речовин, утриманням диких звірів, службових собак та собак бійцівських порід тощо, що створює підвищену небезпеку для особи, яка цю діяльність здійснює, та інших осіб.

Таким чином, хоча, безумовно, сучасне законодавство України визначає роботів лише як об’єктів цивільних прав, проте підстави відзначити необхідність найближчим часом реформування законодавства з урахуванням особливостей такого об’єкта.

На думку автора, перспективність дослідження правового статусу роботів не може зводитися лише до такого вузького підходу без урахування глобальної цифровізації та впровадження технологій штучного інтелекту в різні сфери суспільного життя. Йдеться не лише про використання роботів та робототехніки людиною, а фактично про заміну людини, виконання її функцій різними формами штучного інтелекту у певних сферах суспільного життя (наприклад, керування транспортними засобами, надання юридичних послуг (підготовка позовних заяв, ведення справ про банкрутство), диктор (на китайському телебаченні робот веде програму новин). Отже, можливість та здатність автономного функціонування штучного інтелекту (звичайно, в межах визначених для нього завдань) зумовлює необхідність перегляду статусу роботів та правового регулювання відносин за їх участю.

Науковий інтерес автора цієї статті представляє аналіз ідей та концепцій сучасних дослідників цієї проблематики (О.А. Баранов, М.В. Карчевський, К.О. Хернес, Є.О. Харитонов, О.І. Харитонova та інші), які допускають можливість віднесення роботів до суб’єктів права, та визначення у зв’язку з цим передумов подальшого реформування законодавства та перспектив його розвитку.

На сьогодні існує декілька точок зору з приводу визначення правосуб’єктності роботів зі штучним інтелектом в системі правовідносин. Розглянемо деякі з таких підходів, що представляють найбільший дослідницький інтерес.

Концепція правосуб’єктності робота (як потенційного суб’єкта права) є абсолютно новою, відповідно, в першу чергу, необхідно зрозуміти, чи підпадає такий суб’єкт під існуючу класифікацію або буде абсолютно новим видом суб’єктів.

О.А. Баранов обґрунтовує необхідність визнання роботів зі штучним інтелектом суб’єктами суспільних відносин – “еквівалентами фізичної особи” [6]. Роботи в цьому випадку розглядаються як людиноподібні суб’єкти, які здійснюють людиноподібні дії в процесі відносин з традиційними суб’єктами [7].

Крістофер О. Хернес зазначає, що якщо штучний інтелект повинен нести юридичну відповідальність за свої дії, тоді він повинен мати фізичну, юридичну та цифрову ідентичність, подібну людині. Якщо у штучного інтелекту є ті ж юридичні обов’язки, що і у людини, хіба в нього не повинні бути такі ж юридичні права, як у людини? [8].

Однак, на думку автора, з такою “людиноподібною” ознакою штучного інтелекту погодитися не можна, виходячи з того, що суб’єктом цивільних відносин є не людина, а

фізична особа. А крім фізичної особи, суб'єктами можуть виступати і юридичні особи, і держава, й інші суб'єкти публічного права, які також не є “людиноподібними”. Їхній статус в правовідносинах визначається законодавством з урахуванням їх ознак та функцій. Тому порівнювати людину і робота також не є необхідним.

З концепцією “еквівалента фізичної особи” не погоджуються і Є.О. Харитонов, О.І. Харитонova. Натомість вони пропонують визнати роботів зі штучним інтелектом квазі-юридичною особою. При цьому науковці пропонують включити до переліку видів правосуб'єктності юридичної особи також “кіберздатність”, під якою вони мають на увазі здатність бути активним учасником відносин у ІТ-сфері (укладати договори як користувач, бути учасником соціальних мереж, брати участь в інтерактивних акціях тощо). Кіберздатність може реалізовуватися за допомогою не лише правочинів, а й юридичних вчинків [9].

Прихильники визнання такої правосуб'єктності роботів в якості історичної аналогії наводять приклад саме конструкції юридичної особи, яка ґрунтується на концепції *Persona Ficta* та довгий час вважалася штучною конструкцією. В цьому випадку можна не брати до уваги такі фактори, як наявність або відсутність у робота внутрішньої волі, самосвідомості та інших подібних якостей, які притаманні людині [10].

Враховуючи, що визнання будь-кого суб'єктом права історично було прерогативою та виключною компетенцією держави, то для надання роботам такого статусу необхідно реформування традиційної концепції суб'єктного складу правовідносин, а також внесення відповідних змін до законодавства. Зокрема, потребують правового закріплення та регулювання визначення, ознаки, момент виникнення та припинення правосуб'єктності, її зміст та елементи тощо.

Російські дослідники пропонують введення в науковий обіг поняття “електронна особа”, оскільки це, на думку О.А. Ястребова, обумовлено перш за все специфікою принципово нового суб'єкта права. Дане поняття покликано відобразити його сутність та правову специфіку [11].

Електронна особа може мати схожість з юридичною особою в тому сенсі, що обидві є для їх власників засобом досягнення певної мети та існують і створюються виключно в інтересах їх власників або творців. Робот, будучи наділеним правовим статусом електронної особи, не отримує раптово прав і обов'язків, аналогічних людським, а власник робота створює юридичну фікцію, контроль над якою він здатний здійснювати.

На думку автора статті, така концепція має право на існування та подальший розвиток на підставі Резолюції, про яку вже було згадано вище. Передбачається, що такий правовий статус дозволяє “найдосвідченішим автономним роботам” мати статус електронних осіб, які будуть “відповідальні за виправлення будь-якого збитку, який вони можуть заподіяти”. Можливо, електронна особистість буде застосовуватися до випадків, “коли роботи приймають автономні рішення чи іншим чином взаємодіють з третіми сторонами незалежно” (пункт 59 (f)) [4].

Також до Резолюції було включено ряд положень, що стосуються “відповідальності”. Хоча Європейський Парламент зазначив, що “принаймні на даному етапі відповідальність повинна покладатися на людину, а не на робота” (пункт 56), Парламент все ж закликав Європейську Комісію проаналізувати наслідки юридичного вирішення проблеми “[створити] конкретний правовий статус роботів” в довгостроковій перспективі (пункт 59 (f) Резолюції) [4].

Таким чином, дослідивши зазначені ідеї та концепції науковців у визначеній сфері, автор статті вважає, що найбільш прийнятною для подальшого дослідження та розвитку

із запровадженням в перспективі у законодавство є концепція визначення статусу робота зі штучним інтелектом як електронної особи.

Виходячи з вищенаведеного, можна зазначити наступне.

Оскільки законодавство в досліджуваній сфері лише починає формуватися, то в цій роботі розглянуто не тільки існуючі підходи до правового регулювання в даній сфері, а й викладено пропозиції дослідника на перспективу. Глобальна цифровізація суспільних відносин та масштабне впровадження штучного інтелекту, здатного приймати автономні рішення в межах поставлених завдань, обумовлює необхідність перегляду концепцій правового регулювання відносин у цій сфері. І хоча для пересічних громадян, особливо з віддалених провінційних населених пунктів, може здатися утопією навіть думка про те, щоб “порівняти людину з роботом”, надавати розумним роботам правосуб’єктність, прирівнявши їх в правах з іншими суб’єктами суспільних відносин, однак це не повинно бути перешкодою для подальшого науково-технічного прогресу та еволюції законодавства. Свого часу концепція “юридичної особи” також зазнавала подібної критики, але на сьогодні впевнено зайняла своє місце в цивілістичній науці та знайшла законодавче закріплення.

Висновки.

Досліджуючи існуючі ідеї, концепції та норми законодавства щодо перспектив визначення правового статусу роботів, а також з метою визначення подальших напрямів наукових досліджень в цій сфері, автор вважає важливими такі узагальнення:

1. Питання правосуб’єктності роботів нерозривно пов’язано із визначенням правового статусу як суб’єкта права, оскільки правосуб’єктність є невід’ємною ознакою суб’єкта.

2. Оскільки правосуб’єктність не надається виключно людині, законом вона може бути поширена і на інших суб’єктів, то вважаємо за доцільне розглядати подальшу перспективу розвитку законодавства в напрямку надання роботам особливого суб’єктного статусу – електронної особи.

3. Аналіз чинного законодавства України дає можливість дійти висновку, що саме законодавець визначає суб’єктний склад учасників цивільних відносин, тому надання роботу зі штучним інтелектом статусу електронної особи можливе лише за умови включення відповідної норми до ЦК України та/або спеціального закону.

4. Окремої уваги потребують визначення поняття, змісту, обсягу та елементів правосуб’єктності робота зі штучним інтелектом як електронної особи, а також моменту її виникнення та припинення.

5. Ключове значення для ідентифікації робота зі штучним інтелектом як електронної особи має визначення механізму його державної реєстрації.

6. Наділення роботів зі штучним інтелектом правосуб’єктністю не означає набуття ними прав та обов’язків людини та не повинно бути спрямованим на уникнення відповідальності іншими суб’єктами.

7. При визначенні особливостей правового статусу робота, є підстави припустити, що робот може одночасно виступати як суб’єктом права, так і об’єктом права залежно від характеру правовідносин (наприклад, за аналогією із підприємством, яке, з точки зору цивілістичної науки може бути як об’єктом – цілісним майновим комплексом, так і суб’єктом відносин).

Підсумовуючи наведене вище, необхідно зазначити, що питання визначення правосуб’єктності роботів зі штучним інтелектом є актуальним, але недостатньо дослідженим. Наведені автором висновки не вичерпують визначеної проблематики, є

дискусійними та відкритими для подальшого обговорення науковою спільнотою з метою формування належного правового регулювання в цій сфері.

Використана література

1. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018 – 2020 роки та затвердження плану заходів щодо її реалізації: Розпорядження Кабінету Міністрів України від 17.01.18 р. № 67-р (Концепція, План, Заходи) (*База даних “Законодавство України” / ВР України*). URL: <https://zakon.rada.gov.ua/go/67-2018-%D1%80>
2. New robot strategy, Japan’s Robot Strategy. 10/2/2015. URL: http://www.meti.go.jp/english/press/2015/pdf/0123_01b.pdf
3. Автоматизоване та під’єднане керування: Звіт Комісії з етики Федерального міністерства транспорту і цифрової інфраструктури Німеччини від червня 2017 року. URL: https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.html?nn=12_830; https://www.bmvi.de/SharedDocs/DE/Publikationen/DG/bericht-der-ethik-kommission.pdf?__blob=publicationFile
4. European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics (2015/2103(INL)). URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0051+0+DOC+XML+V0//EN#BKMD-12>
5. Сулин А. Законы о роботах: текущее состояние и тренды. URL: <http://www.comnews.ru/content/106505/2017-03-30/zakony-o-robotah-tekushchee-sostoyanie-i-trendy-aleksey-sulin-upravlya-yushchiy-partner-yuridicheskoy-firmy-axis-pravo>
6. Баранов О.А. Интернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.
7. Баранов О.А. Интернет речей і штучний інтелект: витоки проблеми правового регулювання (частина 2). URL: <http://aphd.ua/publication-377>
8. Christoffer O. Hernæs. Artificial Intelligence, Legal Responsibility and Civil Rights. Aug 22, 2015. URL: <https://techcrunch.com/2015/08/22/artificial-intelligence-legal-responsibility-and-civil-rights>
9. Харитонов Є.О., Харитонova О.І. До проблеми цивільної правосуб’єктності роботів: матеріали наук.-практ. конф. *Інтернет речей: проблеми правового регулювання та впровадження*, м. Київ, 29 листопада 2018 р., НТУУ “КПІ ім. Ігоря Сікорського” / упоряд. В.М. Фурашев, С.О. Дорогих. Київ: Вид-во “Політехніка”, 2018. С. 42-46.
10. Каткова Т.Г. Закони про роботів: сучасний стан і перспективи розвитку URL: <http://aphd.ua/publication-345>
11. Ястребов О.А. Правосубъектность электронного лица: теоретико-методологические подходы. *Труды Института государства и права РАН*. 2018. № 2. URL: <https://cyberleninka.ru/article/n/pravosubektnost-elektronnogo-litsa-teoretiko-metodologicheskie-podhody>
12. Радутний О.Е. Artificial Intelligence (штучний інтелект) та інші загрози (кримінально-правовий вимір). URL: <http://aphd.ua/publication-354>
13. Карчевський М.В. Основні проблеми правового регулювання соціалізації штучного інтелекту. URL: <http://aphd.ua/publication-369>
14. Сидорчук Ю.М. Філософсько-правові проблеми використання штучного інтелекту, URL: http://pravoisuspilstvo.org.ua/archive/2017/3_2017/part_2/6.pdf
15. Фурашев В.М. Интернет речей і право: Интернет речей: матеріали наук.-практ. конф. *Інтернет речей: проблеми правового регулювання та впровадження*, м. Київ, 24 жовтня 2017 р., НТУУ “КПІ ім. Ігоря Сікорського” / упоряд. В.М. Фурашев, С.О. Дорогих. Київ: Вид-во “Політехніка”, 2017. С. 39-43.
16. Фурашев В.М. Право у світлі технології Інтернет-речей: матеріали другої наук.-практ. конф. *Інтернет речей: проблеми правового регулювання та впровадження*, м. Київ, 29 листопада 2018 р., НТУУ “КПІ ім. Ігоря Сікорського” / упоряд. В.М. Фурашев, С.О. Дорогих. Київ: Вид-во “Політехніка”, 2018. С. 29-32.

Правова інформатика

УДК 681.3:004.6+314.1

БРАЙЧЕВСЬКИЙ С.М., кандидат фізико-математичних наук

РЕЗОНАНСНІ ЯВИЩА В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ

Анотація. В роботі розглянуті специфічні ефекти, викликані наявністю двох груп коливних процесів – зміни параметрів оточуючого середовища та обробки вхідних даних системою. Показано, що за певних умов в системі можуть виникати резонансні явища, здатні призводити до її непередбачуваної поведінки.

Ключеві слова: інформаційні технології, Інтернет речей, резонанс.

Summary. The paper deals with specific effects caused by the presence of two groups of oscillatory processes – changes in environmental parameters and processing of input data by the system. It is shown that, under certain conditions, resonance phenomena may occur in the system, which can lead to its unpredictable behavior.

Keywords: information technology, Internet of things, resonance.

Аннотация. В работе рассмотрены специфические эффекты, вызванные наличием двух групп колебательных процессов – изменения параметров окружающей среды и обработки входных данных системой. Показано, что при определенных условиях системе могут возникать резонансные явления, способные приводить к ее непредсказуемому поведению.

Ключевые слова: информационные технологии, Интернет вещей, резонанс.

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 – IoT) [1]. Вони пов'язані з наявністю (принаймні, гіпотетичною) в поведінці систем IoT елементів соціальної поведінки [2]. Питання про природу соціальних відносин між людиною та технологічною системою є, взагалі кажучи, досить нетривіальним. В пропонованій роботі ми не маємо наміру обговорювати цю проблему в повному обсязі.

Ми не торкатимемось питань розумності машини, наявності у неї свідомості тощо. З практичної точки зору важливо те, що сучасні технологічні системи можуть призводити до наслідків, що однозначно не витікають із їх будови та тих задач, які перед ними ставить людина. Через це людина не в змозі відповідати за них. Ці наслідки не мають нічого спільного зі “свободою волі” машини і насправді викликані специфічними особливостями її функціонування. Але вони, по суті, відіграють таку ж роль, як і свідомі дії індивіда. Саме в такому розумінні ми говоримо про необхідність правового регулювання відносин людина – машина.

В пропонованій роботі ми зупинимось лише на одному аспекті проблеми – непередбачуваності поведінки системи, зумовленій нелінійними ефектами в її роботі.

Ми покажемо, що за певних умов в системі IoT можуть виникати резонансні явища, які призводять до непередбачуваних рішень, що приймає система. Йдеться про явище, аналогічне параметричному резонансу, яке зумовлене певним співвідношенням внутрішньої частоти роботи програмного комплексу та частоти зміни зовнішніх параметрів, що

використовуються як вхідні дані. Головна причина такої поведінки полягає в тому, що за рахунок обміну даними між різними компонентами системи IoT через мережу Інтернет, внутрішня частота роботи системи за порядком величини може співпадати з частотою зміни фізичних характеристик зовнішнього середовища.

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

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

Нижче ми проаналізуємо одну з таких можливостей, зумовлену нелінійними ефектами в IoT-системах. А саме, можливість виникнення в них параметричного резонансу (в широкому розумінні).

Нагадаємо, що термін “Інтернет речей” на початку означав концепцію впровадження радіочастотних міток в систему керування логістичними ланцюжками [4; 5]. З часом під IoT почали розуміти концепцію обчислювальної мережі фізичних предметів (“речей”), оснащених вбудованими технологіями для їх взаємодії одне з одним або з оточуючим середовищем [6]. Головна ідея полягала в тому, що використання таких мереж дозволить (принаймні, частково) виключити участь людини. На наш час переважає розуміння IoT як сукупності технічних систем і комплексів, що взаємодіють між собою через мережу Інтернет [1; 3]. Вважається, що концепція IoT в практичній реалізації має як технологічні, так і соціальні наслідки [2].

Метою статті є визначення нелінійної поведінки систем IoT, яка зумовлена наявністю в процесах обробки вхідних даних коливних процесів в умовах періодичної зміни параметрів зовнішнього середовища.

Виклад основного матеріалу. Нижче ми проаналізуємо один із аспектів можливих реалізацій цієї концепції. А саме, внесок в роботу системи IoT нелінійних ефектів, зумовлених резонансними явищами.

Коли ми говоримо про нелінійні ефекти, маємо на увазі те, що система IoT, взагалі кажучи, є нелінійною. Нагадаємо, що нелійними називають динамічні системи (тобто системи, стан яких змінюється в часі), що математично описуються нелінійними рівняннями. Навпаки, лінійні системи – такі, що описуються лінійними рівняннями [7]. Ми не будемо заглиблюватись в теорію нелінійних систем, обмежившись лише деякими загальними зауваженнями..

Строго кажучи, лінійних систем в природі не існує, тому що реальні процеси завжди описуються нелінійними рівняннями. Лінійна система – це свого роду абстракція, в якій лінійні рівняння дають результат, достатньо точний для практичних цілей. Системи, що не допускають такого абстрагування, зустрічаються достатньо рідко. Але часто нелінійність системи стає помітною в практичному плані за певних умов. Тоді кажуть про нелінійні ефекти в такій системі. Ми обмежимося одним з багатьох можливих явищ, пов'язаних з специфічною поведінкою навколишнього середовища системи IoT.

На рівні технологічної реалізації IoT є набором датчиків, що фіксують задані параметри навколишнього середовища, та пристроїв, що обробляють вхідні дані, отримані від датчиків. Для нас суттєво, що обмін даними здійснюється за допомогою мережі Інтернет. Метою створення такої системи є виключення безпосередньої участі людини, принаймні в частині функціональних можливостей системи. Це, в свою чергу, означає, що система IoT повинна на основі обробки отриманих вхідних даних приймати рішення, результатом яких буде реальний вплив на оточуюче середовище. Зрозуміло, що в тих випадках, коли прийняті рішення неадекватні фактичній ситуації, наслідки роботи системи можуть бути вкрай негативними. Як приклад, можемо розглянути протипожежну систему музейних приміщень, яка отримує дані про температуру середовища, швидкість її зміни (це потрібно для визначення загоряння на початковій стадії), концентрацію продуктів згоряння в повітрі тощо. Якщо система помилково визначить критичну ситуацію, вона спрацює, що призведе до блокування приміщення і відкачки повітря. В разі присутності в приміщенні, наприклад, групи екскурсантів, це може мати фатальні наслідки.

Важливим є питання про можливі причини виникнення таких ситуацій. Стандартними вважаються чинники, що утворюють три групи:

- помилки алгоритмів програмного комплексу;
- помилкові вхідні дані;
- невідповідні значення параметрів роботи алгоритмів, які встановлюють експлуатаційники в процесі налаштування системи в конкретних умовах.

Якщо система є лінійною, то незначні відхилення в кожній з груп ведуть до незначних відхилень в поведінці системи як такої. Отже, по-перше, при правильному налаштуванні не виникатиме позаштатних ситуацій, а, по-друге, якщо такі ситуації й виникатимуть, вони не матимуть помітних наслідків. Важливо те, що поведінка лінійної системи прогнозована. Дійсно, знаючи використовувані алгоритми та конкретні значення параметрів, ми можемо покроково пройти весь тракт системи і визначити критичні точки, в яких можуть виникати збої. Тому відповідальність за негативні

наслідки функціонування системи лежить на проектувальниках, виробниках та експлуатаційниках.

Але можуть виникати інші ситуації, в яких поведінка системи стає не прогнозованою, і не існує способу визначити, коли і за рахунок чого відбувся збій. Єдине, що нам доступне – гіпотетично припустити можливість подібної поведінки. В таких випадках має сенс говорити про “відповідальність” машини. Нижче ми обговоримо одну з них, в основі якої лежить явище параметричного резонансу [8 – 10]. Такі явища виникають, коли встановлюється певна відповідність внутрішньої частоти коливної системи та частоти коливань значення її параметра.

Відразу зауважимо, що явища, про які ми будемо говорити нижче, не є параметричним резонансом в стандартному розумінні (як його розуміють у фізиці), оскільки система IoT, строго кажучи, не є осцилятором в класичному значенні цього слова. Маємо лише певні аналогії, які дозволяють моделювати конкретні реальні ситуації. Звичайно, ми будемо використовувати спрощену картину, оскільки реальні системи IoT набагато складніші і з точки зору функціональних задач, і з точки зору технічної реалізації. Наша мета полягає в дослідженні принципових можливостей.

Для такого моделювання нам перш за все потрібно визначити, що є аналогом власної частоти осцилятора. Цей аналог ми і будемо називати внутрішньою частотою системи.

Можливість визначення такого аналога зумовлена тим, що робота програмного комплексу системи IoT завжди є циклічною. В її основі лежить цикл, який здійснює обхід всіх портів, по яких надходять вхідні дані, і виконує їх обробку. Якщо при черговому обході нових даних немає, цикл нічого не робить. Даний цикл може бути “схований” на низькому рівні і керуватися безпосередньо операційною системою, але ця обставина не змінює суті справи. Тому робота системи, незалежно від конкретної реалізації, від початку характеризується певною частотою. Обробка вхідних даних може мати (і, скоріш за все, має) внутрішні цикли, які характеризуються своїми частотами. Суперпозиція цих частот і є аналогом власної частоти класичного осцилятора. Ця частота, очевидно, не пов’язана з фізичним рухом (в тому чи іншому сенсі). Йдеться про періодичну зміну стану системи, але цього достатньо для розуміння специфічних ефектів взаємодії такої системи з оточуючим середовищем.

Наступним кроком є визначення аналога амплітуди коливань системи, з величиною якої, власне, і пов’язане явище резонансу. Ми в цьому плані використовуватимемо змінну (в найпростішому випадку це простий лічильник), величина якої збільшується або зменшується залежно від стану зовнішнього оточення. Оскільки значення даної змінної (будемо називати її контрольною) відбиває стан оточення системи, воно здійснює коливання, в тому числі і за рахунок періодичного обнуління на початку деяких циклів. Тому ця змінна може під обраним нами кутом зору, розглядатися як амплітуда коливань системи. Якщо її значення після завершення чергового циклу досягає певної величини, система спрацьовує в той чи інший спосіб, тим самим виконуючи свою задачу.

Обхід стандартних портів в звичайних комп’ютерних системах здійснюється процесором і тому має достатньо високу частоту, щоб не брати до уваги коливні ефекти. Але в системах IoT ситуація інша. Ключову роль відіграє та обставина, що ці системи є системами з розподіленими параметрами [8 – 9]. Так називають системи, просторові масштаби процесів в яких сумірні з просторовими масштабами зміни фізичних параметрів оточення. Важливо, що стан таких систем визначається функціями кількох незалежних змінних, що, як правило, залежать не лише від часу, а й від просторових

координат. А обмін даними в системах IoT здійснюється через Інтернет, що має кінцеву швидкість передачі сигналу (яка, до того ж, не є сталою через різноманітні технічні чинники).

Отже, маємо такі специфічні особливості роботи систем IoT:

- поточний набір вхідних даних формується за допомогою різних датчиків, які не обов'язково точно синхронізовані, а отже, системі, можливо, доводиться чекати, поки не буде завершено формування повного набору;
- датчики, що визначають градієнти параметрів (швидкості їх зміни), можуть мати помітний час спрацювання;
- наявність вкладених циклів, які обробляють дані від різних комплексів датчиків, і передають результати обробки іншим програмним компонентам;
- обмін даними здійснюється по мережі Інтернет, що також займає певний час, який, до того ж, не є сталим в часі.

Тому реальні проміжки часу отримання і обробки чергової порції вхідних даних може суттєво зростати і досягати значень, сумірних з часовими характеристиками фізичних процесів. Відповідно, і внутрішня частота нашої системи може виявитись достатньо низькою, внаслідок чого резонансні явища стають цілком можливими.

Наприклад, якщо отримання і обробка даних контролю зростання температури оточення буде протягом достатнього часу співпадати з періодичним її зростанням, а періодичне зниження буде ігноруватись, значення контрольної змінної почне необмежено зростати, що викличе спрацювання системи в умовах, для яких воно не передбачене.

Особливість подібної поведінки системи полягає в тому, що виникнення резонансного явища, взагалі кажучи, неможливо спрогнозувати. Неадекватне зростання контрольної змінної викликано не алгоритмами програмного комплексу (вони працюють в штатному режимі) і не значеннями характеристик зовнішнього середовища (вони знаходяться в межах припустимого). Причиною є нелінійні ефекти, викликані особливостями роботи системи, пов'язаними з двома категоріями періодичних процесів – внутрішніх та зовнішніх. Виникнення їх зумовлене саме наявністю розподіленої системи датчиків, які в режимі реального часу постійно формують набори вхідних даних.

Висновки.

Отже, ми бачимо, що за певних умов характер взаємодії IoT з оточуючим середовищем може призводити до нелінійних ефектів з елементами непередбачуваної поведінки системи. Один із можливих випадків пов'язаний з періодичністю зміни параметрів оточення.

Таким чином, суто технологічні властивості системи IoT можуть зумовити її функціонування, що значною мірою моделює власну поведінку. Під власною поведінкою системи ми розуміємо здатність виконувати дії, які не визначаються однозначно її технологічними властивостями. Ця поведінка не впливає з алгоритму, а також з наявних значень показів датчиків і параметрів налаштування. Оскільки системи IoT безпосередньо впливають на перебіг подій в реальних ситуаціях, маємо підстави вважати описані вище явища такими, що містять в собі елемент суспільних відносин. Маємо на увазі, що функціонування технологічних систем в сучасному світі може виходити за рамки однозначного виконання команд людини, і, тим самим, стає елементом суспільних процесів.

Тому, враховуючи можливі негативні для суспільства наслідки, вона може сприйматися як суб'єкт соціальних відносин і підлягати правовому регулюванню. Наприклад, у випадку явної загрози для суспільства, така система може бути демонтована за рішенням суду.

Використана література

1. Баранов О.А. Интернет речей і штучний інтелект: витoki проблеми правового регулювання: зб. матеріалів II-ї міжнародної науково-практичної конф. *IT-право: проблеми та перспективи розвитку в Україні*, м. Львів, 17 лист. 2017 р. Львів: НУ “Львівська політехніка”, 2017. 318 с. С. 18-42.
2. Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений – Структура и функциональные модели архитектуры. Обзор Интернета вещей: Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y. URL: <http://handle.itu.int/11.1002/1000/11559>
3. Баранов О.А. “Интернет речей” як правовий термін. *Юридична Україна*. 2016. № 5 – 6. С. 96-103. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf
4. Леонид Черняк. Платформа Интернета вещей. *Открытые системы. СУБД*. 2012. № 7. 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). <<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”. <<https://www.gartner.com/it-glossary/internet-of-things>>
7. Боулдинг К. Общая теория систем – скелет науки. Москва: Наука, 1969.
8. Мандельштам Л.И. Лекции по теории колебаний. Москва: Наука, 1972.
9. Рабинович М.И., Трубецков Д.И. Введение в теорию колебаний и волн. Москва: Наука, 1984.
10. Магнус К. Колебания. Введение в исследование колебательных систем. Москва: Мир, 1982. 304 с.
11. Бутковский А.Г. Теория оптимального управления системами с распределенными параметрами. Москва: Наука, 1965.

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

УДК 004.7:001.8

ЛАНДЕ Д.В., доктор технічних наук, керівник наукового центру  
НДІП НАПрН України

ДМИТРЕНКО О.О., аспірант, Інститут проблем реєстрації інформації НАН України

РАДЗІЄВСЬКА О.Г., кандидат юридичних наук, старший науковий співробітник  
НДІП НАПрН України

## ПОБУДОВА ОНТОЛОГІЙ В ГАЛУЗІ ПРАВА ЗА ДАНИМИ SERVICE GOOGLE SCHOLAR

**Анотація.** У статті викладені підходи до структуризації даних, розподілених в наукових документальних ресурсах мережі Інтернет. Представлено методи формування моделей предметних галузей як мереж із термінів певної тематики, які є інформаційно важливими в межах заданої теми. Побудовано мережі природніх ієрархій термінів для корпусу документів, пов'язаних з тематиками "Criminal Law" та "Copyright Law". Розглянута у статті методика створення мережі зі слів та словосполучень – алгоритм формування мереж природніх ієрархій термінів сприятиме формуванню й удосконаленню понятійного і термінологічного апарату у правовій сфері та гармонізації національного і міжнародного права.

**Ключові слова:** інформаційні ресурси, правова інформація, термінологія, мережа природної ієрархії термінів, предметна область, онтологія.

**Summary.** The article presents approaches to the structuring of data distributed in scientific documentary resources of the Internet. It represents generating methods of subject branches models as networks in terms of certain subjects, containing important information in the framework of the given topic. Networks of natural hierarchies of terms for the corpus of documents related to the topics "Criminal Law" and "Copyright Law" are built. The considered methodic of creating a network of words and phrases, the implementation of the algorithm for the formation of networks of natural hierarchies of terms – will contribute to the formation and improvement of conceptual and terminological apparatus in the legal sphere and the harmonization of national and international law.

**Keywords:** information resources, legal information, terminology, network of natural hierarchy of terms, subject domain, ontology.

**Аннотация.** В статье изложены подходы к структуризации данных, распределенных в научных документальных ресурсах сети Интернет. Представлены методы формирования моделей предметных областей как сетей из терминов определенной тематики, информационно важных в пределах заданной темы. Построены сети естественных иерархий терминов для корпуса текстовых документов связанных с тематиками "Criminal Law" и "Copyright Law". Рассмотренная в статье методика создания направленной сети со слов и словосочетаний – алгоритм формирования сетей естественных иерархий терминов способствует формированию и совершенствованию понятийного и терминологического аппарата в правовой сфере и гармонизации национального и международного права.

**Ключевые слова:** информационные ресурсы, правовая информация, терминология, сеть естественной иерархии терминов, предметная область, онтология.

**Постановка проблеми.** Глобалізація інформаційного простору та стрімкий розвиток інформаційно-комунікаційних технологій призвели до не менш стрімкого розвитку інформаційних ресурсів. Виникла невідкладна потреба у дослідженнях та розробках нових методів та засобів більш швидкого пошуку та синтезу потрібної інформації, нових підходів до створення ефективних пошукових систем. Також постає питання зручного

візуального представлення отриманої інформації. Сучасний науково-технічний прогрес породжує нові суспільні відносини, а також суттєво трансформує існуючі. Це значно ускладнює процеси своєчасного виявлення найбільш важливих суспільних відносин та встановлення правовідносин. Структуризація даних, розподілені в інформаційних ресурсах, методами формування мереж із текстів певної тематики на основі автоматично екстрагованих ключових термінів, допоможе спростити поставлене завдання та сприятиме формуванню й удосконаленню понятійного і термінологічного апарату у правовій сфері та гармонізації національного і міжнародного права.

Дуже важливим етапом у комплексних дослідженнях є детальне формалізоване представлення знань обраної предметної області (Subject Domain), придатне для автоматизованої обробки – створення онтологій, в тому числі й правових. Процес побудови великих тематичних онтологій зазвичай є складним та ресурсозатратним. Окремий крок такої формалізації – це визначення базових об'єктів (в даному випадку – створення словникових номенклатур, тезаурусів та предметних словників з термінів, визначених на основі тематичних масивів текстових документів). Ефективний вибір окремих термінів й, тим більше, автоматизація такого відбору з текстового масиву – актуальна й невирішена задача [1; 2]. Досліджуючи лексику, яка використовується в певних текстових масивах, за окремими ключовими термінами-маркерами можна визначати відповідність цих текстів до певної тематики загальних інформаційних потоків. Не менш складною й відкритою проблемою концептуалізації є встановлення зв'язків між термінами.

Також виникає питання щодо подальшого візуального представлення предметних областей. Однією із моделей предметних областей може розглядатися мережа слів (Language Network), вузли якої відповідають окремим поняттям, а ребра – зв'язкам між ними [3]. У цій статті описані підходи до формування мережевих структур із корпусу текстових документів на основі вибраних ключових термінів, які є інформаційно важливими в межах обраної теми.

Одним із методів створення термінологічних онтологій є алгоритм формування направленої мережі зі слів та словосполучень – алгоритм формування мереж природніх ієрархій термінів [4] для корпусу текстових документів. Цей алгоритм базується на використанні інформаційно-важливих елементів тексту, опорних слів та словосполучень (уніграм, біграм та триграм) [5], методика виявлення яких представлена в роботі [4]. Алгоритм створення мереж природніх ієрархій термінів передбачає побудову компактифікованого графу горизонтальної видимості [6 – 10] для термів – окремих слів, біграм та триграм, та встановленні направлених зв'язків між термами.

Як зазначено у роботі [11], алгоритм формування мереж природніх ієрархій термінів можна представити у вигляді послідовних етапів, які охоплюють попередню обробку отриманого корпусу текстових документів, виділення ключових слів та словосполучень, що є інформаційно-важливими в межах розглянутої предметної області, побудова компактифікованого графу горизонтальної видимості (CHVG), перерахунок сортування вагових значень виділених термів за обраним ваговим критерієм та вибір із них найбільш вагомих. Кінцевим етапом є безпосереднє формування мережі природніх ієрархій термінів (з'єднання вузлів зв'язками “входження”) та її відображення.

**Метою статті** є побудова мережі природніх ієрархій термінів для корпусу текстових документів тематично пов'язаних з “Criminal Law” та “Copyright Law”.

#### **Виклад основного матеріалу**

**Формування корпусу текстових документів.** Початковим етапом формування мережі термів, пов'язаної з певною предметною областю, є формування корпусу текстових документів. Для проведення досліджень була використана вільна доступна пошукова

система, яка індексує повний текст наукових публікацій – Google Scholar (<https://scholar.google.com>). На цьому етапі було вивантажено анотації перших 385-ти статей за запитом “Criminal Law” та анотації перших 490-та статей за запитом “Copyright Law”.

**Обробка текстових документів та виокремлення ключових термів.** На цьому етапі проводиться процес попереднього лексичного аналізу – розбиття тексту на елементарні одиниці (токени або лєми). Токенізація (лематизація) є зазвичай початковим етапом обробки текстів, адже дає змогу працювати зі словом як з окремою сутністю, при цьому знаючи його контекст [12].

Наступним крок – зважування термів. В якості вагових значень термів, для формування часового ряду в якості функції, яка ставить у відповідність слову число, в даному дослідженні використовується класичний статистичний ваговий показник TF–IDF (з англ. Term Frequency – “частота слова”, Inverse Document Frequency – “обернена частота документа”) [13], хоча це не єдиний можливий для вирішення завдання виділення ключових термів підхід [4]. Цей статистичний ваговий показник використовується для оцінки важливості слів у контексті документа, що є частиною колекції документів чи корпусу [14]. Вага (значимість) слова пропорційна кількості вживань цього слова у документі і обернено пропорційна частоті вживання слова у інших документах колекції. Показник TF–IDF використовується в задачах аналізу текстів та інформаційного пошуку. Його можна застосовувати як один з критеріїв релевантності документа до пошукового запиту [15].

TF – відношення числа входжень обраного слова до кількості слів у документі. Таким чином, оцінюється важливість слова  $t_i$  в межах обраного документа. Термін введений Карен Спарк Джонс [16].

$$TF = \frac{n_i}{\sum_k n_k},$$

де:  $n_i$  – число входжень слова в документ;

$\sum_k n_k$  – загальна кількість слів у документі.

IDF – інверсія частоти, з якою слово зустрічається в документах колекції. Використання IDF зменшує вагу широкоживаних слів.

$$IDF = \log \frac{|D|}{|(d_i \supset t_i)|},$$

де:  $|D|$  – кількість документів колекції;

$|(d_i \supset t_i)|$  – кількість документів, в яких зустрічається слово  $t_i$  (коли  $n_i \neq 0$ ).

Вибір основи логарифму у формулі не має значення, адже зміна основи призведе до зміни ваги кожного слова на постійний множник, тобто вагове співвідношення залишиться незмінним. Іншими словами, показник TF–IDF – це добуток двох множників TF та IDF:

$$TF\text{--}IDF = TF \circ IDF.$$

Більшу вагу TF–IDF отримають слова з високою частотою появи в межах документа та низькою частотою вживання в інших документах колекції.

Беручи до уваги той факт, що в даному дослідженні розглядаються документи, що описують одну предметну область, то для запобігання втрати інформаційно-важливих елементів тексту, опорних слів та словосполучень (біграм та триграм), в якості

статистичного показника важливості терма було використано лише показник TF. Такий вибір пояснюється тим, що терми, які є ключовими для розглянутої предметної області й зустрічаються у більшості документів, матимуть низьке числове значення IDF (отже, і низьким буде числове значення TF-IDF), в той час, коли насправді ці слова є інформаційно-важливими, тобто такими, що визначають структуру тексту.

Також щоб уникнути ситуації, що виникає під час роботи з текстовим корпусом заздалегідь визначеної тематики, коли інформаційно-важливий терм зустрічається майже у кожному документі корпусу і має низький ваговий показник TF, було застосовано глобальний TF-GTF (Global TF) [17].

$$GTF = \frac{n_i}{\sum_k n_k},$$

де:  $n_i$  – загальна кількість появи терма  $i$  у всіх документах корпусу;

$\sum_k n_k$  – загальна кількість термів у документах корпусу.

Цей підхід дозволяє інформаційно-важливим в глобальному контексті елементам тексту мати високий статистичний показник важливості.

**Вилучення стоп-слів.** Також після етапу обробки текстових документів та виокремлення ключових термів в даному дослідженні пропонується вилучити стоп-слова, які не мають ніякого смислового навантаження, тобто є інформаційно-неважливими, а також біграми, які містять принаймні одне стоп-слово, та триграми, які починаються, або закінчуються стоп-словом. Стоп-словник, який використовувався в межах даного дослідження, був сформований на основі різних стоп-словників, які доступні за посиланнями:

<https://code.google.com/archive/p/stop-words/downloads>;

<http://www.textfixer.com/tutorials/common-english-words.php>.

**Процес стематизації.** Для об'єднання (злиття) слів, які мають спільний корінь в даному дослідженні здійснюється процес стематизації – скорочення слова до основи шляхом відкидання допоміжних частин, таких як закінчення чи суфікс [18]. Стематизація або стемінг (англ. – stemming) є процесом нормалізації тексту шляхом знаходження основи слова. Варто зазначити, що основа слова не обов'язково співпадає з морфологічним коренем слова.

Існує декілька типів алгоритмів стемінгу, які розрізняються відносно продуктивності, точності та відносно того, як долаються проблеми стемінгу [19].

Алгоритм стемінгу Мартіна Портера [20; 21] набув значного поширення та став де-факто стандартним алгоритмом стемінгу для англійської мови. Для проведення досліджень було використано стример, що реалізований на мові Python (бібліотека NLTK – Natural Language Toolkit).

Загалом, стемінг застосовується в лінгвістичній морфології та в пошукових системах для розширення пошукового запиту користувача та є частиною нормалізації тесту.

**Алгоритм побудови компактифікованого графу видимості.** У роботах [4; 6 – 8, 22; 23] запропоновано алгоритм побудови мереж термів – алгоритм побудови компактифікованого графу горизонтальної видимості (Compactified Horizontal Visibility Graph – CHVG). Загалом, мережа термів з використанням алгоритму горизонтальної видимості будується у три етапи. На першому етапі на горизонтальній осі позначається ряд вузлів, кожен з яких відповідає словам у тому порядку, в якому вони з'являються в тексті, а по вертикальній осі відкладаються вагові значення – числові оцінки. На

другому етапі будується граф горизонтальної видимості [9; 10]. Більш формально ідею побудови графу горизонтальної видимості можна представити наступним чином: два вузли  $t_i$  і  $t_j$ , які відповідають елементам часового ряду  $x_i$  і  $x_j$ , знаходяться у горизонтальній видимості тоді й тільки тоді, коли

$$x_k < \min\{x_i, x_j\}$$

для всіх  $t_k$  ( $t_i < t_k < t_j$ ).

Третій етап полягає в тому, що отримана на попередніх етапах мережа компактифікується. В результаті буде отримано нову мережу термів – компактифікований граф горизонтальної видимості (CHVG) – Рис. 2.

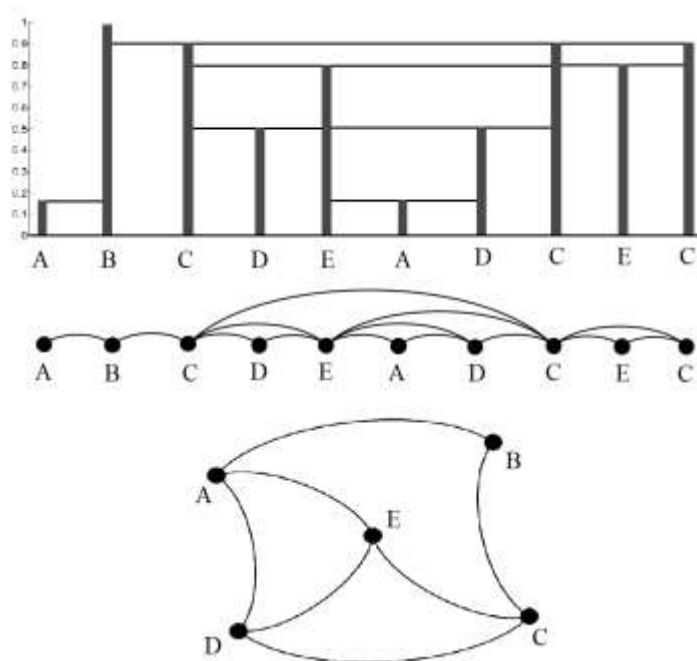


Рис. 1. Етапи побудови компактифікованого графу горизонтальної видимості

**Формування мережі природніх ієрархій термінів.** Для послідовностей термів (слів, біграм та триграм) та їх вагових значень, визначених за допомогою статистичного показника важливості терма – GTF, будуються компактифіковані графи горизонтальної видимості (CHVG).

Наступним кроком є перерахунок вагових значень, що відповідають термам у CHVG. Ця процедура дозволяє врахувати в подальшому також ті терми, які мають велике значення для загальної тематики текстового корпусу [22]. Під час виконання досліджень перерахунок ваг здійснюється з використанням алгоритму HITS [24; 25], завдяки якому визначається авторство чи посередництво для кожного вузла CHVG. Вибір форми вагового значення (авторство чи посередництво) немає значення, оскільки граф є ненаправленим. Після цього всі терми упорядковуються за спаданням розрахованих вагових значень відповідних їм вузлів у CHVG.

Далі експертним методом визначається необхідний розмір (число  $N$ ) створюваної мережі природніх ієрархій термінів, після чого вибирається  $N$  простих слів, біграм та триграм (всього  $N+N+N$  елементів), що мають найбільші значення вагових показників відповідних їм вузлів у CHVG.

На наступному етапі будується сама мережа природніх ієрархій термінів, в якій вузли відповідають відібраним термам, а зв'язки між ними – входженням одного терма в інший (Рис. 2).

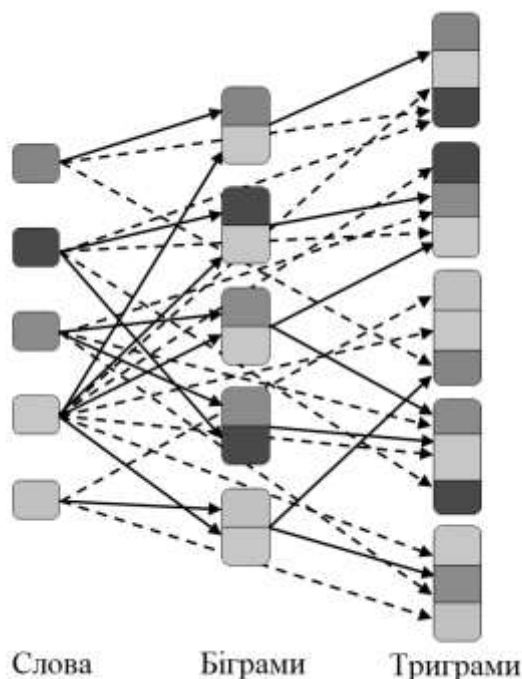


Рис. 2. Трирівнева модель мережі природніх ієрархій термінів

Заключним є відображення створеної мережі природніх ієрархій термінів засобами візуалізації графів. На вхід таким засобом подається матриця інцидентності у форматі csv, створена на етапі формування мережі природніх ієрархій термінів.

Мережа природніх ієрархій термінів, що створюється повністю автоматично, може розглядатися як основа для подальшого автоматизованого формування термінологічних онтологій за участю експертів.

**Візуалізація й аналіз результатів дослідження.** Для проведення досліджень в даній роботі використано корпус заздалегідь вибраних текстових документів, що тематично пов'язані з актуальною предметною областю – “Criminal Law”. Імпортувавши стример, що реалізований на мові Python (бібліотека NLTK – Natural Language Toolkit), було попередньо здійснено процес стематизації текстового корпусу отриманого для запиту “Criminal Law” об'ємом 385 документи, внаслідок чого слова, які мають спільний корінь, були об'єднанні.

У Табл. 1 наведені списки найбільш вагомих термів (слів, біграм та триграм) для досліджуваної предметної області відповідно до мережевого рангового критерію HITS [24; 25].

Таблиця 1. Списки найбільш вагомих термів (слів, біграм та триграм) для “Criminal Law”

| № | Слова | Біграми         | Триграми             |
|---|-------|-----------------|----------------------|
| 1 | studi | restor_justic   | civil_and_crimin     |
| 2 | moral | onlin_librari   | heinonlin_thi_articl |
| 3 | work  | law_reform      | crimin_law_doctrin   |
| 4 | law   | crimin_sanction | law_and_crimin       |

|    |           |                     |                         |
|----|-----------|---------------------|-------------------------|
| 5  | principl  | columbia_law        | theori_of_crimin        |
| 6  | respons   | crimin_respons      | crimin_law_text         |
| 7  | subject   | civil_law           | univers_of_pennsylvania |
| 8  | liabil    | univers_press       | american_crimin_justic  |
| 9  | human     | corpor_crimin       | crime_and_crimin        |
| 10 | right     | gener_principl      | case_and_materi         |
| 11 | intern    | articl_examin       | analysi_of_crimin       |
| 12 | role      | case_involv         | intern_and_compar       |
| 13 | concept   | mental_disord       | principl_of_crimin      |
| 14 | gener     | compar_crimin       | substant_crimin_law     |
| 15 | univers   | court_icc           | american_crimin_law     |
| 16 | examin    | crimin_justic       | crimin_court_icc        |
| 17 | practic   | feder_crimin        | crime_against_human     |
| 18 | polici    | substant_crimin     | field_of_crimin         |
| 19 | year      | intern_crimin       | sanctiti_of_life        |
| 20 | theori    | crimin_code         | philosophi_of_crimin    |
| 21 | crime     | war_crime           | columbia_law_review     |
| 22 | review    | common_market       | crimin_law_theori       |
| 23 | case      | compar_law          | law_sj_schulhof         |
| 24 | develop   | paper_examin        | law_and_criminolog      |
| 25 | legal     | sexual_violenc      | journal_of_intern       |
| 26 | heinonlin | law_review          | crime_and_punish        |
| 27 | articl    | intern_law          | english_crimin_law      |
| 28 | public    | social_scienc       | role_of_crimin          |
| 29 | social    | intern_crime        | law_and_procedur        |
| 30 | histori   | law_theori          | crimin_law_case         |
| 31 | court     | american_law        | intern_crimin_justic    |
| 32 | author    | soviet_crimin       | wiley_onlin_librari     |
| 33 | procedur  | crimin_liabil       | crimin_law_defens       |
| 34 | american  | crimin_procedur     | intern_crimin_court     |
| 35 | major     | crimin_tribun       | crimin_law_volum        |
| 36 | discuss   | crimin_law          | crimin_law_enforc       |
| 37 | question  | feder_court         | harvard_law_review      |
| 38 | prosecut  | intern_commun       | pennsylvania_law_review |
| 39 | crimin    | law_journal         | crimin_and_civil        |
| 40 | issu      | secur_council       | crim_l_criminolog       |
| 41 | edit      | law_enforc          | compar_crimin_law       |
| 42 | societi   | law_doctrin         | intern_crimin_law       |
| 43 | defens    | american_crimin     | crimin_law_review       |
| 44 | enforc    | american_journal    | journal_of_law          |
| 45 | punish    | human_right         | intern_crimin_tribun    |
| 46 | doctrin   | militari_tribun     | yale_law_journal        |
| 47 | feder     | mental_disabl       | feder_crimin_law        |
| 48 | justic    | crimin_court        | crimin_law_reform       |
| 49 | problem   | common_law          | corpor_crimin_liabil    |
| 50 | rule      | prosecutori_discret | heinonlin_crimin_law    |

Використовуючи засоби програмного забезпечення для моделювання та візуалізації графів – Gephi (<https://gephi.org>) [26] побудована мережа природніх ієрархій термінів розміром 50+50+50 була візуалізована (Рис. 3).



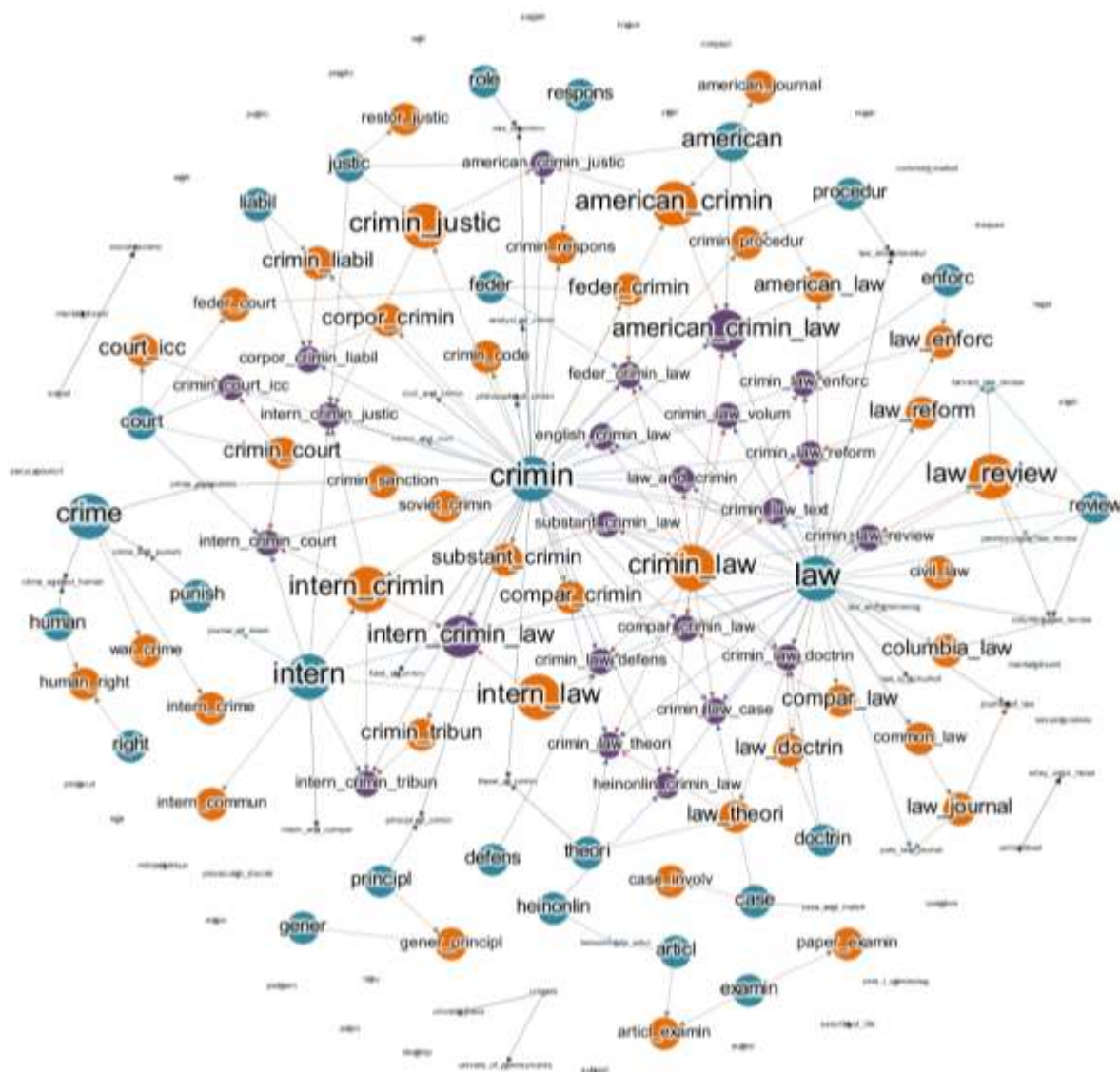


Рис. 3. Мережа природніх ієрархій термінів розміром 50+50+50 для предметної області “Criminal Law”

Також за допомогою засобів програмного забезпечення Gephi були отримані такі параметри створеної мережі: кількість вузлів – 150; кількість зв'язків – 205; щільність мережі – 0.009; кількість зв'язаних компонент – 35; середня довжина шляху – 1; середній коефіцієнт кластеризації – 0.121.

За топологічною особливістю побудована мережа має малий середній коефіцієнт кластеризації. Це пояснюється наявністю в мережі великої кількості понять, сусіди яких мало пов'язані один з одним – це є ознакою так званих квазіієрархічних мереж. Невелика середня довжина шляху свідчить про те, що ця мережа також є “малим світом” (Small World) [27].

Також було досліджено корпус текстових документів, що тематично пов'язані з актуальною предметною областю – “Copyright Law”. Попередньо здійснено процес стематизації корпусу, що був отриманий для запиту “Copyright Law”, обсягом 490 документи.

В Табл. 2 наведені списки найбільш вагомих термів (слів, біграм та триграм) для досліджуваної предметної області відповідно до мережевого рангового критерію HITS.

*Таблиця 2. Списки найбільш вагомих термів (слів, біграм та триграм)  
для “Copyright Law”*

| №  | Слова      | Біграми              | Триграми                          |
|----|------------|----------------------|-----------------------------------|
| 1  | digit      | copyright_legisl     | type_of_tumour                    |
| 2  | intellectu | digit_technolog      | wiley_onlin_librari               |
| 3  | unit       | properti_right       | author_and_publish                |
| 4  | music      | copyright_protect    | heinonlin_thi_articl              |
| 5  | work       | cardozo_art          | fair_use_doctrin                  |
| 6  | law        | law_reform           | german_copyright_law              |
| 7  | origin     | violat_fall          | law_in_canada                     |
| 8  | public     | canadian_copyright   | soc_y_usa                         |
| 9  | fair       | three-step_test      | access_to_copyright               |
| 10 | protect    | unauthor_copi        | case_and_materi                   |
| 11 | properti   | legal_studi          | law_of_copyright                  |
| 12 | patent     | intel_prop           | intellectu_properti_right         |
| 13 | right      | intellectu_properti  | purpos_of_copyright               |
| 14 | intern     | copyright_handbook   | law_and_econom                    |
| 15 | creativ    | univers_press        | professor_of_law                  |
| 16 | analysi    | berkeley_tech        | literari_and_artist               |
| 17 | current    | digit_media          | digit_millennium_copyright        |
| 18 | gener      | paid_violat          | law_jc_ginsburg                   |
| 19 | inform     | copyright_law        | patent_and_copyright              |
| 20 | nation     | copyright_work       | canadian_copyright_law            |
| 21 | internet   | septemb_9            | law_is_base                       |
| 22 | theori     | copyright_owner      | law_a_commentari                  |
| 23 | question   | subject_matter       | aspect_of_copyright               |
| 24 | copi       | public_domain        | public_or_part                    |
| 25 | artist     | intern_copyright     | librarian_and_educ                |
| 26 | case       | part_thereofispermit | law_of_septemb                    |
| 27 | develop    | current_copyright    | notion_of_origin                  |
| 28 | author     | special_case         | european_copyright_law            |
| 29 | media      | copyright_limit      | transit_ma_schlossbauer           |
| 30 | econom     | law_review           | republ_of_china                   |
| 31 | legal      | digit_millennium     | analysi_of_copyright              |
| 32 | industri   | american_copyright   | intellectu_properti_law           |
| 33 | creat      | exclus_right         | paid_violat_fall                  |
| 34 | articl     | german_copyright     | nation_inform_infrastructur       |
| 35 | social     | copyright_infring    | protect_by_copyright              |
| 36 | court      | copyright_case       | law_and_practic                   |
| 37 | publish    | european_copyright   | heinonlin_copyright_law           |
| 38 | american   | unfair_competit      | approach_to_copyright             |
| 39 | number     | wto_panel            | law_c_geiger                      |
| 40 | art        | digit_copyright      | version_and_permiss               |
| 41 | materi     | open_sourc           | american_copyright_law            |
| 42 | univers    | law_journal          | digit_copyright_law               |
| 43 | copyright  | properti_law         | current_copyright_law             |
| 44 | technolog  | moral_right          | springer-verlag_berlin_heidelberg |
| 45 | societi    | copyright_fee        | berlin_heidelberg_gmbh            |
| 46 | softwar    | copyright_soc        | law_a_propos                      |

|    |           |                 |                        |
|----|-----------|-----------------|------------------------|
| 47 | cultur    | copyright_issu  | law_p_samuelson        |
| 48 | heinonlin | price_discrimin | intern_copyright_law   |
| 49 | limit     | current_version | dichotomi_in_copyright |
| 50 | futur     | law_school      | guid_to_copyright      |

Використовуючи засоби програмного забезпечення для моделювання та візуалізації графів – Gerhi побудована мережа природніх ієрархій термінів розміром 50+50+50 була візуалізована (Рис. 4).

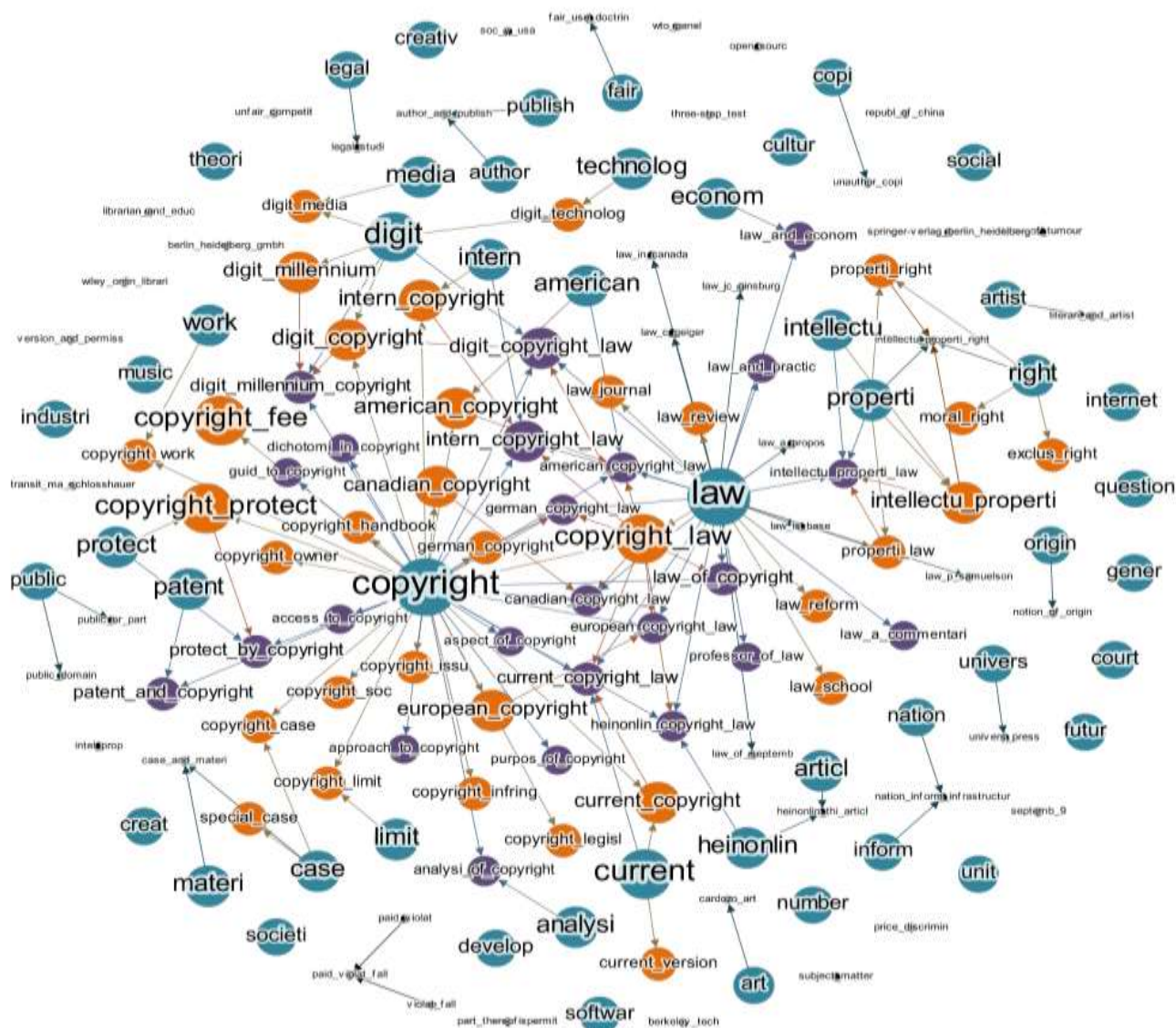


Рис. 4. Мережа природніх ієрархій термінів розміром 50+50+50  
для предметної області “Copyright Law”

Також за допомогою засобів програмного забезпечення Gephi були отримані такі параметри створеної мережі: кількість вузлів – 150; кількість зв'язків – 144; щільність мережі – 0.006; кількість зв'язаних компонент – 48; середня довжина шляху – 1; середній коефіцієнт кластеризації – 0.068.

## Висновки.

У статті розглянуто методику створення мережі зі слів та словосполучень – алгоритм формування мереж природніх ієрархій термінів для масиву тематично пов'язаних текстових документів. Розглянута методика була застосована для створення

моделей предметних областей “Criminal Law” та “Copyright Law”. На основі найбільшої вільно-доступної пошукової системи, яка індексує повний текст наукових публікацій – Google Scholar, були попередньо підготовлені текстові корпуси за запитом “Criminal Law” та “Copyright Law” об’ємом 385 документів та 490 документи відповідно. Були отримані мережі природних ієрархій термінів для масиву текстових документів тематично пов’язаних з “Criminal Law” та “Copyright Law”.

В якості допоміжних інструментів для дослідження були використаний пакет візуалізації та моделювання графів Gephi (<http://gephi.org>) та власний набір спеціально розроблених модулів на мові програмування Python. Було встановлено, що створені мережі за топологічною особливістю мають малий середній коефіцієнт кластеризації. Невелика середня довжина шляху підтверджує припущення про те, що ця мережа є “малим світом” (Small World).

Отже, мережа природної ієрархії термінів, що створюється повністю автоматично, може розглядатися як основа для подальшого автоматизованого формування термінологічних онтологій за участю експертів. Розглянута у статті методика створення направленої мережі зі слів та словосполучень сприятиме формуванню й удосконаленню понятійного і термінологічного апарату у правовій сфері та гармонізації національного і міжнародного права. Також результати дослідження можуть бути використані під час створення персональних пошукових інтерфейсів користувачів інформаційно-пошукових систем, що, в свою чергу, дозволить спростити процес пошуку необхідної інформації.

### Використана література

1. Лукашевич Н.В., Добров Б.В., Чуйко Д.С. Отбор словосочетаний для словаря системы автоматической обработки текстов. *Компьютерная лингвистика и интеллектуальные технологии: труды международной конференции “Диалог – 2008”*. Москва, 2008. С. 339-344.
2. Филиппович Ю.Н., Прохоров А.В. Семантика информационных технологий: опыты словарно-тезаурусного описания. Москва: МГУП, 2002. – 368 с.
3. Ланде Д.В. Элементы компьютерной лингвистики в правовой информатике. Київ: НДПП НАПрН України, 2014. 168 с.
4. Lande D.V., Snarskii A.A., Yagunova E.V., and Pronoza E. The Use of Horizontal Visibility Graphs to Identify the Words that Define the Informational Structure of a Text. In: *Proceedings of the 12th Mexican International Conference on Artificial Intelligence*, 2013. Pp. 209-215.
5. Yagunova E.D. and Lande D.V. Dynamic Frequency Features as the Basis for the Structural Description of Diverse Linguistic Objects. *CEUR Workshop Proceedings. Proceedings of the 14th All-Russian Scientific Conference “Digital libraries: Advanced Methods and Technologies, Digital Collections”*. Pereslavl-Zalessky. Russia, 2012. Pp. 150-159.
6. Wang M., Xu H., Tian L. and Stanley H.E. Degree distributions and motif profiles of limited penetrable horizontal visibility graphs. *Physica A: Statistical Mechanics and its Applications*. 2018.
7. Wang M., Vilela A.L., Du R., Zhao L., Dong G., Tian L., and Stanley H.E. Exact results of the limited penetrable horizontal visibility graph associated to random time series and its application. *Scientific reports*. 8(1). 2018.
8. Wang M., Vilela A.L., Du R., Zhao L., Dong G., Tian L., and Stanley H.E. Topological properties of the limited penetrable horizontal visibility graph family. *Physical Review E*. 97(5), 2018.
9. Luque B., Lacasa L., Ballesteros F., and Luque J. Horizontal visibility graphs: Exact results for random time series. *Physical Review E*. 80(4). 2009.
10. Gutin G., Mansour T., and Severini S. A characterization of horizontal visibility graphs and combinatorics on words. *Physica A*. 390. 2011. Pp. 2421-2428.
11. Lande D.V. Building of Networks of Natural Hierarchies of Terms Based on Analysis of TextsCorpora. E-preprint ArXiv 1405.6068.

12. Manning C.D., Raghavan P., and Schütze H. An Introduction to Information Retrieval. *Cambridge University Press*. 2009. Pp. 22-36.
13. Salton G. and Buckley C. Term-weighting approaches in automatic text retrieval. *Information Processing & Management*. № 24(5). 1998. Pp. 513-523.
14. Ullman J.D. Data Mining, Mining of massive datasets. *Cambridge University Press*. 2011. Pp. 1-17.
15. Beel J., GIPP B., Langer S., Breitingen C. Research-paper recommender systems: a literature survey. *International Journal on Digital Libraries*. 17(4). 2016. Pp. 305-338.
16. Jones K.S. A statistical interpretation of term specificity and its application in retrieval. *Journal of Documentation, MCB University Press*. 60. 2004. Pp. 493-502.
17. Lande D.V., Dmytrenko O.O., Snarskii A.A. Transformation texts into complex network with applying visibility graphs algorithms. *Інформаційні технології та безпека: матеріали XVIII Міжнародної научно-практичної конференції ІТБ-2018*. Київ: ООО “Інжиніринг”. 2018. С. 20-33. CEUR Workshop Proceedings (ceur-ws.org). Vol-2318 urn:nbn:de:0074-2318-4. Selected Papers of the XVIII International Scientific and Practical Conference on Information Technologies and Security (ITS 2018).
18. Jongejan B., and Dalianis H. Automatic training of lemmatization rules that handle morphological changes in pre-, in- and suffixes alike. In the *Proceeding of the ACL-2009*. Joint conference of the 47th Annual Meeting of the Association for Computational Linguistics and the 4th International Joint Conference on Natural Language Processing of the Asian Federation of Natural Language Processing. Singapore. August 2-7, 2009. Pp. 145-153.
19. Baeza-Yates R., Ribeiro B. D. A. N. Modern information retrieval. New York: ACM Press. Harlow. England: Addison-Wesley. 2011.
20. Porter M.F. An algorithm for suffix stripping. *Program*. Vol. 14. No. 3. 1980. Pp. 130-137,
21. Willett P. The Porter stemming algorithm: then and now. *Program: Electronic Library and Information Systems*. Vol. 40. No 3. 2006. Pp. 219-223.
22. Lande D.V., and Snarskii A.A. Compactified HVG for the Language Network. In: *Proceedings of the International Conference on Intelligent Information Systems: The Conference is dedicated to the 50th anniversary of the Institute of Mathematics and Computer Science*. 20-23 Aug. 2013, Chisinau, Moldova: Proceedings IIS, Institute of Mathematics and Computer Science. 2013. Pp. 108-113.
23. Lande D.V., Snarskii A.A., and Yagunova E.V. Application of the CHVG-algorithm for scientific texts. In: *Proceedings of the Open Semantic Technologies for Intelligent Systems (OSTIS)*, February 20 – 22th. Minsk. 2014. Pp. 199-204.
24. Kleinberg J.M. Authoritative sources in a hyperlink environment. *Journal of the ACM JACM*. 46 (5). 1999. Pp. 604-632.
25. Langville A.N., and Meyer C.D. Google’s PageRank and beyond: the science of searchengine rankings. Princeton university press. 2011.
26. Cherven K. Network Graph Analysis and Visualization with Gephi. Packt Publishing, 2013.
27. Kleinberg J. Navigation in a small world. *Nature*. 2000. 406 (6798). P. 845.

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


Інформаційна і національна безпека

УДК 340+35.078.3

ДОВГАНЬ О.Д., доктор юридичних наук, старший науковий співробітник,
НДІ інформатики і права НАПрН України
ТКАЧУК Т.Ю., кандидат юридичних наук, доцент,
ННІ інформаційної безпеки НА СБ України

**КОНЦЕПТУАЛЬНІ ЗАСАДИ ЗАКОНОДАВЧОГО ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ**

Анотація. У статті досліджується концептуальні засади правового забезпечення інформаційної безпеки України. На основі теоретичного аналізу запропоновано модель Закону України “Про інформаційну безпеку України” та проаналізовано основні його змістовні частини.

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

Summary. The article deals with the conceptual principles of the legal providing of Ukraine's information security. On the basis of theoretical analysis, the model of the Law of Ukraine “On Information Security of Ukraine” is proposed and its main content parts are analyzed.

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

Аннотация. В статье исследуются концептуальные основы правового обеспечения информационной безопасности Украины. На основе теоретического анализа предложена модель Закона Украины “Об информационной безопасности Украины” и проанализированы основные его содержательные части.

Ключевые слова: информационная безопасность, обеспечение информационной безопасности, национальная безопасность, система, состояние, процесс, угроза.

Постановка проблеми. Не викликає сумніву, що будь-яке законодавство має спиратися на чітку, науково обґрунтовану й об’єктивно зумовлену систему права. Тому систематизація інформаційного законодавства потребує створення стрункої комплексної галузі інформаційного права, формування положень, котрі втіляться в конкретні норми законів та підзаконних нормативно-правових актів. А отже розробка й удосконалення вітчизняного законодавства з безпекових питань інформаційної сфери мають відбуватися на міцному теоретичному фундаменті, науковому обґрунтуванні місця в загальній системі права підгалузі правового забезпечення інформаційної безпеки, а також її взаємодії з іншими правовими галузями та інститутами.

Слід зазначити, що теперішній стан захищеності прав і законних інтересів людини, суспільства й держави в інформаційній сфері України свідчить про недостатній рівень правового регулювання й забезпечення інформаційної безпеки. Так, непоодинокими є випадки порушення чи безпідставного обмеження вказаних прав та інтересів, у нормах, що регулюють інформаційні відносини, у правовому забезпеченні інформаційної безпеки існує чимало суперечностей, лакун і колізій, а деякі відносини у цій сфері

взагалі не врегульовані. Убачається, що все це зумовлене насамперед слабким теоретичним обґрунтуванням підгалузі правового забезпечення інформаційної безпеки та іншими системними прорахунками. Стосовно цієї підгалузі спостерігаємо також розсинхронізацію між системами права й законодавства, усунення якої потребує системного підходу до відповідної законотворчості. Саме такий підхід має стати головним методологічним інструментом забезпечення інформаційної безпеки, оскільки за його допомогою можливе розв'язання проблем співвіднесення цілого й частини, організації та дезорганізації, порядку й безладу.

Ефективності інформаційного законодавства в цілому серйозно шкодить також відсутність у нормативно-правових актах з питань забезпечення інформаційної безпеки єдиних для всіх джерел правового регулювання відповідних засадничих нормативних умов.

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 О. Баранова [1], Н. Нижника, Г. Ситника та В. Білоуса [2], В. Брижка [3], Є. Захарова та Р. Тополевського [4], В. Пилипчука [5], П. Сніцаренка, Ю. Сарачива, В. Семененка та В. Ткаченка [6], О. Яреми [7] та ін.

Метою статті є визначення концептуальних засад правового забезпечення інформаційної безпеки України на теперішньому етапі, з урахуванням сучасних загроз та євроатлантичної інтеграції нашої держави, та запропонувати модель проекту Закону України “Про інформаційну безпеку України”.

Виклад основного матеріалу. Поряд із юридичними конструкціями, правилами та прийомами викладення законодавчих та інших нормативно-правових актів чи не найважливішим засобом юридичної техніки є відповідна термінологія. Система визначень, що характеризує різні аспекти інформаційної діяльності, стає основою формування відповідних безпекових понять, необхідних для розвитку технологій організації і забезпечення інформаційної безпеки. А між тим, термінологія, що застосовується у сфері забезпечення інформаційної безпеки, демонструє на брак єдності, неоднозначні тлумачення, а то й узагалі відсутні визначення багатьох понять, у тому числі ключових. Усе це створює серйозні перешкоди як для правотворчої діяльності в інформаційній сфері, так і для правозастосовної, а також зайвий раз засвідчує відсутність системності у розв'язанні вказаних проблем.

Наприклад, до теперішнього часу немає законодавчого визначення такого базового терміна як “безпека інформації”, хоча таке термінологічне сполучення вживається в деяких законах. У Законі України “Про основи національної безпеки”, який був основним орієнтиром забезпечення безпеки України, системна сутність безпеки інформації трактувалася як невід’ємна складова національної безпеки України, не даючи при цьому її точного визначення. Крім того, в цьому Законі замість поняття “інформаційна безпека України” використовувався термін “національна безпека України в інформаційній сфері”. Визначення поняття “інформаційна безпека”, різні за своєю суттю і в Законах України “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” та “Про телекомунікації”. У більшості наукових праць з питань інформаційної безпеки здебільшого розглядаються суто технічні питання захисту інформації: захист інформаційно-телекомунікаційних систем, каналів передачі інформації, доступ до інформації, розробка засобів захисту баз даних, захист від витоку інформації тощо.

У Законі України “Про основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” [8], *“інформаційна безпека”* визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Проте, слід враховувати, що даний правовий акт розроблявся і був прийнятий до початку явних проявів гібридної війни, і по-друге, на наше переконання даному підходу притаманний однобічний підхід до забезпечення інформаційної безпеки. З врахуванням міжнародного досвіду ми пропонуємо також включати у зміст даного поняття заходи активної оборони.

Проект Закону про внесення змін до законів України щодо інформаційної безпеки, в якому пропонується доповнити Закон України “Про національну безпеку України” визначенням *“інформаційна безпека”* [9], значною мірою повторює зазначене вище поняття *“інформаційна безпека”*, проте дещо розширює спектр негативного впливу, зокрема вже згадується інформаційно-психологічний вплив. Проте, як і в попередньому, воно займає більш оборонний характер, дещо нівелюючи активні заходи забезпечення інформаційної безпеки України.

Ми визначаємо інформаційну безпеку України як стан, за якого в умовах дії реальних та потенційних загроз забезпечується самозбереження, сталий і прогресивний розвиток інформаційної сфери, зокрема захищеність інформаційної інфраструктури, інформаційного простору, інформаційних ресурсів, інформаційних процесів та їх суб’єктів, а також досягнення відповідних національних цілей та реалізація національних інтересів в інформаційній сфері. При цьому забезпечення інформаційної безпеки держави, на нашу думку, це постійний процес діяльності компетентних органів, спрямований на запобігання, протидію загрозам інформаційній сфері, застосування активних заходів інформаційного впливу, а також сукупність умов такої діяльності, які реалізуються і здатні контролюватися тривалий час.

В основу даного підходу покладено принцип, відповідно до якого основною метою забезпечення інформаційної безпеки є створення безпечного інформаційного середовища. А для цього захищати національні інтереси й цінності, виходячи з виявлення загроз і намірів противника, замало. Даний підхід передбачає також протидію та активні контрзаходи у процесі забезпечення інформаційної безпеки держави.

Контекстний аналіз вживання законодавця поняття *“безпека інформації”* дає підстави тлумачити його як стан захищеності інформації в системі. Відповідно, *“захист інформації”* – це діяльність із забезпечення вказаного стану захищеності. Захист інформації як складова діяльності із забезпечення безпеки інформації та інформаційної безпеки є одним із засобів захисту прав і законних інтересів людини, суспільства, держави в інформаційній сфері.

Найбільш точно, на нашу думку, цей процес можна відобразити в категоріях *“захист”* і *“охорона”*, які разом охоплюють діяльність із забезпечення інформаційної безпеки. Суть охорони інформації полягає у встановленні щодо окремих її видів певного правового режиму, скажімо, державної таємниці. Натомість захист інформації – це сукупність заходів із протидії загрозам та протиправним посяганням на права та законні інтереси суб’єктів в інформаційній сфері.

Важливою складовою інформаційної безпеки вбачається комплексний захист зазначених прав і законних інтересів від непередбачуваного й шкідливого впливу

певного інформаційного техніко-технологічного середовища, створеного самим соціумом, тобто від побічних чинників впливу технологічних та організаційних процесів на особу (людину і громадянина), суспільство, державу. При цьому система інформаційної безпеки покликана нейтралізувати вказані негативні впливи на людину та сприяти підтриманню стабільності суспільства й держави, інститути котрої, у свою чергу, повинні цю нейтралізацію забезпечити. Іншими словами, головною ознакою стану захищеності в інформаційній сфері (інформаційної безпеки) є оптимальне співвідношення інтересів людини, суспільства й держави.

Чинниками забезпечення інформаційної безпеки держави є гарантування:

- 1) безпеки інформації загального доступу, мереж зв'язку, інформаційно-телекомунікаційних систем, технічних та програмних засобів виконання маніпуляцій з інформацією, доступу до інформації;
- 2) конфіденційності інформації з обмеженим доступом;
- 3) захищеності особи, суспільства й держави від шкідливого впливу певних видів інформації (в даному разі йдеться не про інформацію, віднесену до категорій з обмеженим доступом, а про такі її види, котрі здатні зашкодити вказаним суб'єктам інформаційних відносин).

На сьогодні зазначені відносини, пов'язані із забезпеченням інформаційної безпеки, далеко не повно законодавчо врегульовані. Можна констатувати лиш загальну регламентацію діяльності щодо захисту інформації. Саме тлумачення змісту поняття “захист інформації” вважаємо не зовсім коректним, позаяк однією із цілей цієї діяльності називається фактично самозабезпечення – захист інформації спрямований на забезпечення захисту інформації, що утруднює не тільки розуміння змісту діяльності, а й оцінювання її результатів. Тому метою цієї діяльності, на наш погляд, слід визнати досягнення стану безпеки інформації як складової інформаційної безпеки.

Описане вище становище спричинене відсутністю сформульованих в одному законі концептуальних аспектів забезпечення інформаційної безпеки держави. При цьому зазначимо, що для розробки такого закону належить виокремити джерела права, котрі містять норми, які відповідають даному інституту, на основі створеної в системі права підгалузі правового захисту інформаційної безпеки. Ці норми, сьогодні розпорошені по багатьох галузевих законах і до того ж нерідко суперечать одна одній.

В умовах, у яких нині опинилася Україна через гібридну агресію Російської Федерації, особливої актуальності набуває протидія поширенню шкідливої для психіки людини інформації, яку без перебільшення можна вважати інформаційною зброєю, а також розвиток відповідного законодавства. У цьому контексті інформаційно-психологічну безпеку можна визначити як стан захищеності від окремих осіб та/або певних груп, а також відповідних життєво важливих інтересів людини, суспільства й держави в інформаційній сфері.

Під негативним інформаційно-психологічним впливом ми розуміємо такий вплив на особу чи групу осіб, який здійснюється на їх психіку, зокрема й усупереч їхній волі, із застосуванням спеціальних засобів і методів, що призводить до шкідливих для людини, суспільства та держави наслідків.

Усю глибину загрози подібних постійних, цілеспрямованих, продуманих і щедро фінансованих впливів з боку РФ Україна повною мірою відчула під час анексії Криму та воєнних дій на сході. Убачається, що всі питання, пов'язані із зазначеними впливами, слід передбачити в межах спеціального закону стосовно забезпечення інформаційної безпеки.

Інша проблема, яка потребує законодавчого визначення та врегулювання, – відсутність систематизації законодавства з питань протидії екстремізму в інформаційній сфері. Внаслідок цього матеріали подібного змісту часто розповсюджуються практично безперешкодно, позаяк діяльність із запобігання й припинення різних видів екстремізму здійснюється компетентними державними органами безсистемно й нерідко формально.

При цьому важливо пам'ятати, що реальна протидія екстремістським чи іншим негативним проявам в інформаційній сфері не повинна перетворюватися на зведення особистих рахунків з “незручними” журналістами, тиск на опозиційні засоби масової інформації та придушення свободи слова.

Таким чином, вважаємо за доцільне з метою чіткого системного врегулювання питань протидії інформаційному екстремізму, що забезпечило б захист законних інтересів людини від негативних інформаційних впливів, суспільної моралі та держави, а також задля усунення колізій і прогалин законодавства регламентувати зазначену діяльність окремим законом з питань забезпечення інформаційної безпеки.

З цього приводу, наприклад, О. Ярема зазначає, що для інституційного розвитку правового забезпечення інформаційної безпеки необхідно прийняти Закон України “Про інформаційну безпеку” [7, с. 250].

Єдності щодо шляхів якісної трансформації інформаційного законодавства України дослідники цієї проблематики допоки не досягли, що не дивно з огляду на складність, динаміку та масштабність сучасних інформаційних процесів, які відбуваються в умовах становлення національної правової системи [7, с. 252].

Одна з основних причин невідповідності інформаційного законодавства України вимогам сучасності є те, як слушно зазначається у [2, с. 89] – те, що у суспільній і науковій думці не сформувався цілісне уявлення про інформаційну безпеку з позиції права та юридичної науки.

Життєдіяльність інформаційного суспільства потребує чіткого законодавчого врегулювання багатоманітних відносин, що виникають у зв'язку зі створенням, функціонуванням, використанням інформаційних систем і ресурсів, каналів комунікацій, відповідних технологій тощо. Досліджене у попередніх працях формування в системі інформаційного права такої підгалузі, як правове забезпечення інформаційної безпеки, зумовлює потребу виокремлення законодавчих актів, положень, норм, котрі регламентують різні аспекти забезпечення інформаційної безпеки, їхнього аналізу на предмет наявності системних вад, а також систематизації, консолідації на цій основі загальних правових норм у єдиний базовий закон, позбавлений існуючих у теперішній час суперечностей, колізій та прогалин. Це, у свою чергу, має створити передумови для якісної комплексної трансформації законодавства, яке регулює інформаційні відносини в різних сферах життєдіяльності суспільства. Ідеться передусім про прийняття Закону України “Про інформаційну безпеку України”.

Зауважимо, що ідея розробки такого закону не є новою, а найбільш результативні спроби її реалізації припадали на 2004 та 2014 роки.

Так, у 2004 році був розроблений проект Закону України “Про інформаційну безпеку України” (від 22 вересня 2004 року № 5732). Фактично зазначений законопроект становив лише словник визначень, що стосуються інформаційної безпеки (ст. 2); перераховував її об'єкти (ст. 3) та суб'єкти (ст. 4); зазначав підстави гарантування державою цілісності інформаційного простору (ст. 5); наводив перелік загроз інформаційному простору й інформаційній безпеці (не розрізняючи їх та не передбачаючи можливості виникнення нових загроз) (ст. 6); загальними фразами окреслював шляхи забезпечення інформаційної безпеки України (ст. 7); визначав

основні напрями державної політики в інформаційній сфері (ст. 9). Відтак, за оцінками експертів, “законопроект справляє враження навчального посібника, присвяченого чи то теорії інформаційної безпеки, чи то інформаційному простору” [4].

Приміром, у ст. 10 “Система забезпечення інформаційної політики та інформаційної безпеки України” систематизовано й наведено повноваження Президента України, Верховної Ради України, Ради національної безпеки і оборони України, Кабінету Міністрів України, міністерств, Служби безпеки України, інших центральних органів виконавчої влади, місцевих державних адміністрацій, органів місцевого самоврядування, правоохоронних органів, судів загальної юрисдикції, Генеральної прокуратури України; окремі права громадян в інформаційній сфері. Вочевидь, закріплення таких норм, які відтворюють уже закріплені законодавчо положення лишень з наголосом на повноваження зазначених суб’єктів в інформаційній сфері, не тільки не врегульовує відповідні суспільні відносини, але й створює можливість обмеження діяльності у сфері інформаційної безпеки виключно наведеними повноваженнями. При цьому значна частина статей законопроекту має бланкетний характер і відсилає до норм чинного законодавства, що аж ніяк не сприяє визначеності правового регулювання.

Фактично законопроект був спрямований на фіксацію рамкових засад інформаційної безпеки і мав переважно декларативний характер. Відсутність конкретизації й орієнтація на загальні положення прийнятна, скажімо, для Концепції забезпечення інформаційної безпеки, але аж ніяк не для закону. Складність і багатоманітність інформаційних відносин зумовлюють необхідність систематизації нормативно-правових актів стосовно інформаційної сфери у вигляді, наприклад, Інформаційного кодексу (статті, присвячені правовому регулюванню інформаційної безпеки, могли би скласти окремий розділ чи книгу цього кодексу) або Закону України “Про інформацію”, викладеного в новій редакції.

З огляду на зазначені вище та інші істотні вади проект закону “Про інформаційну безпеку України” було знято з розгляду.

Така ж сама доля спіткала і його більш сучасного “наступника” – проект закону “Про засади інформаційної безпеки України” (реєстр. № 4949 від 28 травня 2014 року) [10]. У цьому законопроекті пропонувалося визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, порядок забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, а також закріпити правові основи інформаційної безпеки України.

Фахівці Головного науково-експертного управління Апарату Верховної Ради України в узагальнюючому висновку від 19 червня 2014 року, погоджуючись з необхідністю врегулювання порушених у законопроекті питань, зауважили, що чимало його положень потребують доопрацювання й уточнення для їх узгодження з іншими законодавчими актами з питань інформаційної безпеки і боротьби з комп’ютерною злочинністю та наповнення конкретним нормативним змістом.

Так, у законопроекті застосовувалася нова для вітчизняного законодавства термінологія. Це, зокрема, поняття “інформаційна безпека”, “інформаційна сфера”, “кібернетична безпека (кібербезпека)”, “кібернетичний простір (кіберпростір)” та низка інших тематичних термінів. Однак при цьому лишилося незрозумілим, чому “інформаційна безпека” тлумачиться як “стан захищеності...”, а “кібернетична безпека” – як “здатність людини...”. Адже визначення цих споріднених термінів, котрі, очевидно,

співвідносяться між собою як загальне та спеціальне, має ґрунтуватися на одних і тих же вихідних поняттях.

Хоча поняття “кіберзлочинність” і пов’язана з ним термінологія, використовується досить широко, офіційного, закріпленого в міжнародних документах та національному законодавстві його визначення досі не існує. Навіть Конвенція про кіберзлочинність 2001 року і Додаткові протоколи до неї [11] оперують поняттями “комп’ютерна система”, “комп’ютерні дані” та передбачають встановлення відповідальності за “правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передачу комп’ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп’ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп’ютерної системи” тощо. Тож запропоновані в законопроекті терміни, зокрема “кіберзлочинність” і “кібертероризм”, не узгоджувалися з термінологією, що вже використовується в чинному законодавстві.

Зміст терміна “кібертероризм”, крім того, охоплюється поняттям “технологічний тероризм”, під яким, зокрема, розуміються “злочини, що вчиняються з терористичною метою із застосуванням... засобів електромагнітної дії, комп’ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об’єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру” (ст. 1 Закону України “Про боротьбу з тероризмом” [12]).

Деякі поняття, такі як “об’єкти критичної інформаційної інфраструктури держави”, “кібервійська”, “кіберпідрозділи” (ст. 5 законопроекту), взагалі не отримали визначень, хоча їхній зміст не є загальнозрозумілим.

До наведених у ст. 3 законопроекту принципів забезпечення інформаційної безпеки, які зведені здебільшого до конституційних гарантій права на інформацію, слід було би додати обов’язкове вжиття заходів щодо інформування про небезпеку та захисту журналістів, які працюють у місцях збройних конфліктів та вчинення терористичних актів, а також при ліквідації небезпечних злочинних груп.

Не можемо погодитися і з тим, що лише створення іншими державами кібервійськ чи кіберпідрозділів є підставою для віднесення цих подій до переліку загроз інформаційній безпеці України. Адже нести загрозу чи завдати державі величезної шкоди може навіть одна людина, котра володіє відповідними знаннями й технічними можливостями.

Зміст ст. 6 проекту, що визначає пріоритети державної політики у сфері інформаційної безпеки, мав би узгоджуватися зі ст. 4, де йдеться про життєво важливі інтереси в інформаційній сфері. На наш погляд, вказані поняття споріднені, а тому автори законопроекту оперують у цих статтях ідентичними положеннями. Зокрема, в обох випадках наголошується на необхідності забезпечення конституційних прав і свобод людини і громадянина в інформаційній сфері; забезпеченні (захисту) інформаційного суверенітету; недопущенні несанкціонованого втручання (забезпечення захисту) у зміст, процеси обробки, передачі та використання персональних даних; розвитку інформаційного суспільства в Україні; збереженні та примноженні духовних, культурних і моральних (національних) цінностей українського народу.

Ст. 7, яка визначає основні напрями діяльності держави у сфері забезпечення інформаційної безпеки, також переважана приписами декларативного змісту. Так, в ній відтворюються деякі положення попередніх статей проекту (4 і 6), зокрема, вже

втретє вказується на необхідності “забезпечення неухильного додержання конституційних прав і свобод людини в інформаційній сфері”, “формування вітчизняної індустрії високотехнологічної інформаційної продукції (послуг)”, “демократичного контролю за діяльністю суб’єктів забезпечення інформаційної безпеки” тощо. Крім того, дев’ять абзаців цієї статті починаються зі слів “удосконалення”, “посилення”, “поліпшення”, “розширення”, що свідчить про ненормативний характер відповідних положень, у результаті чого законопроект фактично перетворюється на своєрідну концепцію інформаційної безпеки України. Адже приписів про те, яким чином буде здійснюватися відповідне “удосконалення”, “посилення” чи “розширення”, документ не містить.

У ст. 8, де називаються об’єкти інформаційної безпеки, вкотре наголошується на необхідності забезпечення “конституційних прав і свобод людини і громадянина, на захищеності від негативного впливу інформаційних технологій та інформаційно-психологічного впливу” (статті 4, 6, 7). Уважаємо, що кількаразове відтворення одного й того ж положення, навіть дуже важливого, в одному законопроекті є очевидною техніко-юридичною помилкою.

Чимало питань виникає і щодо статусу запропонованого до створення аналізованим документом центрального органу виконавчої влади зі спеціальним статусом у сфері інформаційної безпеки – Національної комісії, що здійснює державне регулювання з питань інформаційної безпеки (далі – Нацкомісія інформбезпеки) (ст. 10). Це не повною мірою узгоджується з чинним законодавством, котре визначає порядок створення та формування персонального складу центральних органів виконавчої влади зі спеціальним статусом.

Таким чином, ретроспективний огляд спроб реалізації ідеї щодо розробки єдиного установчого нормативно-правового акту – закону з питань інформаційної безпеки дозволяє дійти висновку, що сьогодні такий закон має чітко визначати сферу правового регулювання, засадничі принципи забезпечення інформаційної безпеки, основні загрози правам та інтересам людини, суспільства й держави, котрі цим законом охороняються, зміст і пріоритетні напрями державної політики у цій сфері та засоби її реалізації, перелік та компетенцію органів державної влади, що забезпечують різні складові інформаційної безпеки. Законом мають також передбачатися правові основи цих складових – захисту державної та іншої таємниці, інформації з різними правовими режимами, персональних даних, а також відповідальності за правопорушення в цій сфері. Нарешті, закон має уніфікувати й удосконалити понятійний апарат і термінологію регульованої сфери, оскільки в теперішній час із цим спостерігаються чималі проблеми.

Ми погоджуємося із фахівцями, що причиною непевного стану щодо забезпечення інформаційної безпеки України стало те, що до сьогодні, незважаючи на конституційну норму, ще не прийнято рамкового закону, яким би стверджувалися основні поняття і положення щодо інформаційної безпеки держави. Це загалом гальмує об’єднавчі процеси та забезпечення їх адекватності як в теоретичному руслі, так і в напрямках практики [6].

Теоретичне обґрунтування вказаного закону має спиратися на сформовану у структурі вітчизняної системи права самостійну підгалузь – правове забезпечення інформаційної безпеки, а також відповідну законодавчу підгалузь, положення якої нині містяться в багатьох законодавчих актах різних галузей. Тому головним завданням законодавця вбачається, як уже зазначалося, саме систематизація й усунення наявних недоліків цих норм і положень з урахуванням комплексної природи вказаної підгалузі права та її взаємодії з іншими правовими галузями і структурними утвореннями. Тобто,

належить виявляти правові джерела не лише забезпечення інформаційної безпеки, а й законодавчих актів, котрі взаємодіють з цією підгалуззю, з метою формування стрункої, позбавленої внутрішніх суперечностей системи відповідного законодавства.

Спробуємо змоделювати структурно-змістову схему пропонованого закону.

Розділ 1. Має розкривати найзагальніші питання, зокрема: мета та сфера дії цього закону; основні поняття (терміни), що в ньому вживаються; принципи забезпечення інформаційної безпеки, його суб'єкти та об'єкти; перелік актів законодавства, котрі цю сферу регулюють; загальна структура законодавства про інформаційну безпеку.

Зрозуміло, що положення цієї глави (як і закону загалом) мають відповідати Конституції України, Доктрині інформаційної безпеки України, а також міжнародно-правовим нормам і принципам.

Мета закону – правове регулювання діяльності із забезпечення інформаційної безпеки держави, тобто стану захищеності й балансу інтересів суб'єктів інформаційної сфери – людини, суспільства, держави.

Понятійний, термінологічний апарат цього системоутворювального закону має бути систематизованим й уніфікованим, містити коректно сформульовані визначення. Убачається за потрібне поряд з іншими визначити такі поняття, як: “інформаційна безпека держави”, “захист інформації”, “безпека інформації”, “інформаційно-психологічна безпека”, “стандарты інформаційної безпеки”, “шкідливий (негативний) інформаційний вплив”, “методи й засоби шкідливого інформаційного впливу” та інші. Чинником успішного виконання цього непростого наукового завдання є “проходження у професійній рефлексії юридичного явища від простого знакового заміщення до власне поняття як знаннєвої конструкції. Цей процес на початковому етапі збігається з юридичною діяльністю, юридичною практикою й відокремлюється від неї в результаті професійної рефлексії, дослідження права”. Тому ретельний семантико-змістовий аналіз кожного терміна чи термінологічного сполучення, що включаються до понятійного апарату, специфіки їх уведення в науковий обіг та практики вживання в чинному законодавстві є обов'язковою умовою при розробці закону.

Об'єкт правового регулювання закону – відносини, які складаються у зв'язку з виникненням загроз і викликів правам і законним інтересам суб'єктів цих відносин в інформаційній сфері. Зокрема, це стосується й інформаційного впливу на психіку людини, людську й суспільну свідомість.

Суб'єкти правового регулювання закону – людина, суспільство, держава; органи державного управління, до компетенції яких входить забезпечення інформаційної безпеки; особа, права та/чи законні інтереси котрої в інформаційній сфері були в будь-який неправомірний спосіб порушені.

Щодо загальної структури законодавства, котре регулює сферу інформаційної безпеки, закріплення якої в даному законі вбачається вельми важливим. Системоутворювальним, базовим законодавчим актом має бути власне сам закон про інформаційну безпеку. Позаяк решта законів не повинні суперечити базовому, його прийняття означатиме потребу ретельного вивчення чинного законодавства й приведення його у відповідність.

Уважаємо, що засадничими положеннями побудови вказаного закону, як і діяльності із забезпечення інформаційної безпеки, мають стати такі принципи:

пріоритет прав і свобод людини і громадянина (цей закріплений у міжнародному праві принцип, що віддзеркалює сутність та межі діяльності із забезпечення інформаційної безпеки, є основоположним; у Доктрині інформаційної безпеки України

дотримання прав і свобод людини в інформаційній сфері віднесене до першорядних національних інтересів нашої країни);

збалансованість інтересів особи, суспільства та держави (цей принцип також передбачений Доктриною інформаційної безпеки України й впливає із першого, позаяк законність інтересів кожної людини простягається до меж прав і свобод інших людей, а також інтересів суспільства й держави, якраз і зумовлених потребою захисту від посягань на ці права і свободи. Адже саме цим урешті-решт спричинені обмеження, пов'язані, приміром, з охороною державної таємниці, захистом персональних даних тощо);

відповідність безпекових заходів ступеню загроз (також впливає із попереднього принципу. Для запобігання загрозам в інформаційній сфері та їх усунення належить застосовувати заходи, адекватні їх реальному рівню, з мінімально необхідним обмеженням прав і свобод громадян);

монополія держави на розробку й виготовлення спеціальних засобів інформаційного, в тому числі інформаційно-психологічного, впливу (в умовах агресії РФ це означає заборону в Україні певної шкідливої інформації, певних антигуманних інформаційно-психологічних технологій, які цілком слушно багатьма правниками називаються інформаційною зброєю);

прозорість, гласність і контроль громадянського суспільства у сфері забезпечення інформаційної безпеки (тобто, відповідно до Закону України “Про доступ до публічної інформації” будь-які відомості про діяльність органів державного управління, місцевого самоврядування щодо забезпечення інформаційної безпеки мають бути відкритими й доступними для ознайомлення громадян, якщо тільки вони не становлять державну чи іншу передбачену законом таємницю);

обов'язковість залучення до діяльності із забезпечення інформаційної безпеки громадських організацій (реалізація цього принципу, котрий впливає із попереднього та принципу збалансованості інтересів людини, суспільства й держави, дає змогу шляхом громадської оцінки законопроектів, пов'язаних з інформаційною сферою, значно повніше враховувати інтереси різних верств населення, підвищити якість відповідного законодавства).

Загрози інформаційній безпеці. Їх перелік наведено в Доктрині інформаційної безпеки України, й він цілком, на наш погляд, відповідає реаліям сьогодення. Якщо визначати їх у цілому, то це – сукупність чинників, котрі можуть призвести до порушення прав і свобод громадян, а також законних інтересів людини, суспільства й держави в інформаційній сфері.

Розділ 2. Загальні засади функціонування державної системи забезпечення інформаційної безпеки. Тут слід визначити пріоритетні завдання у цій сфері, головним із яких убачається створення й удосконалення відповідного законодавства. На його основі має бути сформована вказана система задля неухильного втілення уповноваженими державними органами законодавчих вимог у цій сфері. Функції координації цієї діяльності доцільно покласти на Службу безпеки України.

Окрім виконання охоронних завдань, діяльність державних органів у цій сфері має бути спрямована на збереження й розширення єдиного інформаційного, духовного, мовного простору України, традицій українського народу й суспільної моралі, розвиток правової свідомості й культури населення стосовно інформаційної безпеки, просвіту громадян з питань безпечного користування інформаційними технологіями, захисту від шкідливих інформаційних впливів тощо.

Основні функції державних органів у досліджуваній сфері впливають із наведених вище завдань. Це насамперед: захист інформаційних систем і ресурсів держави, таємних відомостей та іншої інформації з обмеженим доступом; виявлення фактів шкідливих інформаційних впливів та суб'єктів, що їх здійснюють, нейтралізація та припинення їх протиправної діяльності; розробка нових і вдосконалення існуючих методів і засобів запобігання та протидії загрозам інформаційній безпеці людини, суспільства, держави; організація чіткого функціонування дозвільної, експертної та контрольної систем у вказаній сфері; стандартизація галузі; технічна, правова та інша підготовка висококваліфікованих фахівців з питань забезпечення інформаційної безпеки; розвиток продуктивного міжнародного співробітництва з питань інформаційної безпеки, приведення вітчизняного законодавства у відповідність до міжнародно-правових актів у цій сфері тощо.

Задля реалізації державної політики у сфері забезпечення інформаційної безпеки відповідно до наведених вище принципів, завдань і функцій має бути створена ефективна державна система. Крім уповноважених державних органів, її мають складати науково-дослідницькі, науково-технічні установи, проектні, конструкторські та інші організації, котрі провадять наукові дослідження й розробляють технічні засоби, а також освітні заклади, які займаються підготовкою, перепідготовкою та підвищенням кваліфікації відповідних кадрів. Узгоджені дії вказаних суб'єктів забезпечуються шляхом ліцензійної, сертифікаційної, експертної та контрольної діяльності уповноважених на це органів у сфері забезпечення інформаційної безпеки, формування державних замовлень на відповідні наукові дослідження, освітні та інші послуги тощо.

Комплекс засобів, що їх застосовує державна система інформаційної безпеки, має гарантувати належний її рівень, у тому числі убезпечити суспільство від шкідливих інформаційно-психологічних впливів. Не останню роль у цьому має відіграти згадуване вище ліцензування, основні аспекти якого, зокрема умови отримання ліцензії, слід, на нашу думку, передбачити в базовому законі. Так, необхідною умовою отримання ліцензії вбачається сертифікація методів і засобів, які застосовуються під час проведення діяльності, пов'язаної з інформаційною безпекою.

Що стосується шкідливих інформаційних впливів, то достеменно виявити їх можна лише шляхом спеціальної експертизи. Остання проводиться для виявлення загроз інформаційній безпеці за державними стандартами й за дорученням відповідно уповноважених державних органів.

Допускається також заявний порядок проведення таких експертиз, тому варто, на нашу думку, закріпити окремий механізм розгляду вказаних запитів громадян. Зокрема, проведення подібної державної експертизи доцільно включити до необхідних заходів надання реабілітаційної допомоги людині, котра зазнала шкідливого інформаційно-психологічного впливу.

Необхідним елементом державної системи забезпечення інформаційної безпеки має також бути ефективний контроль за її достатністю та ефективністю, а також за дотриманням законності в усіх аспектах її функціонування.

Розділ 3. Загальні питання забезпечення безпеки інформації з обмеженим доступом: підстави та принципи віднесення відомостей до категорії інформації з обмеженим доступом (таємна, службова інформація, конфіденційна), види інформації з обмеженим доступом (державна, для службового користування, персональні дані, комерційна та ін. види інформації за змістом); загальні засади захисту інформації з обмеженим доступом.

Розділ 4. Загальні питання захисту відкритої (загальнодоступної) інформації від протиправних маніпуляцій з нею (викривлення, приховування, блокування тощо), зокрема: засади та вимоги до захисту інформації в загальнодоступних державних мережах; інформаційно-правові аспекти (на відміну від цивільно-правових) захисту об'єктів інтелектуальної власності (державна реєстрація, акредитація тощо) та ін.

Розділ 5. Загальні засади захисту від недостовірної та шкідливої інформації, негативного інформаційно-психологічного впливу. Тут варто, на наш погляд, зазначити загрози суб'єктам інформаційних відносин, спричинені застосуванням спеціальних методів і засобів інформаційно-психологічного впливу, зокрема: маніпулювання особистісною та суспільною свідомістю, навіювання хибних думок і провокування неправильних дій, завдання шкоди здоров'ю та життю людини тощо.

Виходячи із принципу монополії держави на застосування методів і засобів інформаційно-психологічного впливу, треба передбачити вичерпний перелік підстав, коли воно може бути правомірним, а саме:

1) без відома об'єктів інформаційно-психологічного впливу (у надзвичайних ситуаціях (*стихійні лиха, катастрофи техногенного чи іншого характеру тощо*) – для рятування людей, ліквідації наслідків та ін.; під час воєнних дій проти зовнішнього агресора, проведення антитерористичних, миротворчих операцій);

2) за згодою об'єктів інформаційно-психологічного впливу (з науковою метою (*психічні, психологічні дослідження тощо*); під час підготовки фахівців (*які застосовують методи і засоби психологічного впливу; чия діяльність пов'язана з екстремальними та надзвичайними ситуаціями; які займаються антитерористичною діяльністю; з інформаційної безпеки*)).

Крім того, вбачається доцільним врегулювати питання захисту громадян, суспільства й держави від розповсюдження недостовірної інформації на шкоду їхнім законним інтересам (*наприклад, матеріали вітчизняних та зарубіжних засобів масової інформації, спрямовані на дискредитацію окремих осіб, підлив суспільної злагоди, дестабілізацію ситуації у країні і т.п.*). Слід передбачити право постраждалого суб'єкта на компенсацію завданої шкоди (*моральної та/чи матеріальної*) та публічне спростування недостовірних відомостей, а також порядок його реалізації.

Розділ 6. Загальні питання протидії інформаційному екстремізму. Необхідно визначити вичерпний перелік чітких критеріїв, за якими інформація визнається екстремістською (що загрожує конституційному ладу України), зокрема, умисел суб'єкта її розповсюдження, конкретні умови оприлюднення тощо. Підкреслимо важливість чіткого формулювання вказаних критеріїв, аби уникнути багатозначності їх тлумачення, що може призвести до фактичного запровадження цензури. Належність інформації до екстремістської має встановлюватися спеціальною експертизою, питання щодо організації та проведення якої теж мають бути врегульовані цим законом.

Розділ 7. Види відповідальності за правопорушення, пов'язані зі сферою інформаційної безпеки. Слід передбачити випадки застосування кожного з видів відповідальності – дисциплінарної, цивільно-правової, адміністративної, кримінальної.

Джерела та порядок фінансування діяльності із забезпечення інформаційної безпеки. Додамо, що обсяги бюджетного фінансування залежатимуть, зокрема, від того, чи буде створений спеціальний управлінський орган для керування державною системою забезпечення інформаційної безпеки або ж ці функції розподілятимуться між існуючими владними інститутами.

Висновки.

Підсумовуючи міркування стосовно запропонованої моделі закону, зазначимо, що прийняття базового Закону України “Про інформаційну безпеку України” вбачається необхідним задля консолідації, вдосконалення відповідного законодавства, чіткої структуризації системи нормативно-правових актів у цій галузі, усунення наявних суперечностей, лакун та інших вад.

Цей закон має, на наш погляд, закріпити найзагальніші положення, які поширюватимуться на решту нормативно-правових актів у цій галузі, а саме: принципи правового забезпечення, структуру відповідного законодавства, єдині параметри правового забезпечення інформаційної безпеки, єдину термінологію.

Крім того, вказаний закон, синтезувавши норми підгалузі правового забезпечення інформаційної безпеки, може стати одним із базових при кодифікації вітчизняного законодавства у сфері інформації та створенні Інформаційного кодексу України.

Зрозуміло, що подальша розробка вказаного закону потребує клопіткого теоретичного осягнення, вивчення великих масивів різногалузевих матеріалів, залучення до цієї роботи провідних правників, наукових установ, досвідчених практиків. На заключних етапах для створення якісного нормативно-правового акта законодавець має продемонструвати справжнє юридичне мистецтво, “завданням якого є відшліфування правового матеріалу” [13, с. 34]. Тому проведені вище дослідження правової природи феномену правового забезпечення інформаційної безпеки, місця у вітчизняній системі права цього утворення (підгалузі), норми котрого мають скласти основний зміст майбутнього закону про інформаційну безпеку, вбачається вельми актуальним і корисним.

У свою чергу, такий закон має стати основою для інших нормативних актів у сфері забезпечення інформаційної безпеки, а також керівних документів державної політики в інформаційній сфері та процесу стратегічного планування забезпечення інформаційної безпеки України.

Використана література

1. Баранов О.А. Базовий принцип інформаційного права – забезпечення інформаційної безпеки. *Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти*: матеріали наук.-практ. конф. м. Київ, 6 жовт. 2016 р. / упоряд. В.М. Фурашев. Київ: Вид-во “Політехніка”. 2016. С. 29-35.
2. Нижник Н.Р., Ситник Г.П., Білоус В.Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): навчальний посібник. Ірпінь : Акад. ДПС України, 2000. 304 с.
3. Брижко В.М. Основи систематизації інформаційного законодавства: теоретичні та правові засади: монографія. Київ: ТОВ “Пан-Тот”, 2012. 304 с.
4. Тополевський Р., Захаров Є. Коментарі до проекту Закону України “Про інформаційну безпеку України” від 22.09.04 р. № 5732. URL: <http://khpg.org/index.php?id=1105737155> (дата звернення: 05.03.2019).
5. Пилипчук В.Г. Актуальні питання захисту прав, свобод і безпеки людини в сучасному інформаційному суспільстві. *Проблеми захисту прав людини в інформаційному суспільстві*: збірник матеріалів наук.-практ. конф. / упорядн. Фурашев В.М., Петряев С.Ю. (НДІП НАПрН України, НІСД, Секретаріат Уповноваженого Верховної Ради України з прав людини, НТУУ “КПІ”). Київ: Вид-во “Політехніка”. 2016. С. 6-8.
6. Снідаренко П.М., Саричев Ю.О., Семененко В.М., Ткаченко В.А. Удосконалення чинного інформаційного законодавства України як необхідна умова адекватності заходів щодо забезпечення інформаційної безпеки держави. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського*. 2018. № 2(63). С. 68-74.

7. Ярема О.Г. Предмет правового забезпечення інформаційної безпеки в інформаційному праві. *Науковий вісник Львівського державного університету внутрішніх справ. Серія Право.* 2016. № 2. С. 244-252.

8. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. URL: <http://zakon5.rada.gov.ua/laws/show/537-16> (дата звернення: 05.03.2019).

9. Про внесення змін до законів України щодо інформаційної безпеки: проект Закону України від 26.11.18 р. № 9340. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=65011 (дата звернення: 05.03.2019).

10. Про засади інформаційної безпеки України: проект Закону України від 28.05.14 р., реєстр. № 4949. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=51123 (дата звернення: 05.03.2019).

11. Конвенція про кіберзлочинність. URL: http://zakon0.rada.gov.ua/laws/show/994_575 (дата звернення: 05.03.2019).

12. Про боротьбу з тероризмом: Закон України від 20.03.03 р. URL: <http://zakon5.rada.gov.ua/laws/show/638-15> (дата звернення: 05.03.2019).

13. Рудольф фон Иеринг. Юридическая техника / сост. А.В. Поляков. Москва: Статут, 2008. 231 с.

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

УДК 343.9:343.346.8:004

**ГРЕБЕНЮК М.В.**, кандидат юридичних наук, доцент,  
Міжвідомчий науково-дослідний центр з проблем боротьби  
з організованою злочинністю при РНБО України  
**ЛЕОНОВ Б.Д.**, доктор юридичних наук, старший науковий співробітник,  
Національна академія Служби безпеки України

## **АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЕЛЕКТОРАЛЬНИХ ПРОЦЕСІВ: АНАЛІЗ ЗАРУБІЖНОГО ДОСВІДУ**

**Анотація.** У статті аналізується зарубіжний досвід забезпечення інформаційної безпеки електоральних процесів. Висвітлюються проблеми боротьби з фейковими аккаунтами та деструктивною пропагандою у вітчизняному інформаційному просторі. Аналізуються законодавчі ініціативи США та окремих країн ЄС у сфері забезпечення інформаційної безпеки.

**Ключові слова:** інформаційна безпека, електоральні процеси, деструктивна пропаганда.

**Summary.** The article analyzes the foreign experience of ensuring the information security of electoral processes. The problems of combating fake accounts and destructive propaganda in the domestic information space are covered. Analysis the legislative initiatives of the United States and EU countries in the field of information security is provided.

**Keywords:** information security, electoral processes, destructive propaganda.

**Аннотация.** В статье анализируется зарубежный опыт обеспечения информационной безопасности электоральных процессов. Освещаются проблемы борьбы с фейковыми аккаунтами и деструктивной пропагандой в отечественном информационном пространстве. Анализируются законодательные инициативы США, а также отдельных стран ЕС в области обеспечения информационной безопасности.

**Ключевые слова:** информационная безопасность, электоральные процессы, деструктивная пропаганда.

**Постановка проблеми.** Відповідно до Доктрини інформаційної безпеки України забезпечення інформаційного суверенітету, запобігання інформаційної агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб є пріоритетним завданням політикуму нашої країни [1]. Інформаційна безпека визначається як стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого відбувається завдання шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Напередодні проведення президентських та парламентських виборів в Україні у 2019 році тематика інформаційної безпеки набуває надзвичайної актуальності з огляду на загрозу з боку РФ втручатися у хід та підсумки електоральних процесів з метою дестабілізації політичної ситуації. Не виключається, що РФ буде активно втручатися у виборчий процес в Україні, використовуючи різні засоби, починаючи від дезінформації і закінчуючи кібератаками. Тому на особливу увагу заслуговує захист виборчої системи, об'єкти якої залишаються досить уразливими. Йдеться, зокрема, про можливість злому електронних скриньок та витоку персональних даних ключових кандидатів у президенти, особливо тих, хто серйозно загрожує Кремлю [3].

У серпні 2018 року СБ України заблокувала діяльність мережі Інтернет-агітаторів, яких спецслужби РФ залучили для втручання у майбутні вибори. Російські спецслужби залучили до “співпраці” жителів Дніпра, Кривого Рогу і Нікополя, які є адміністраторами груп в соціальних мережах та поставили завдання з підготовки “плацдарму” для проведення заздалегідь запланованих заходів впливу на хід майбутніх президентських виборів шляхом маніпулювання громадською думкою Інтернет-користувачів. Також з метою маніпулювання свідомістю пересічних громадян спецслужби РФ з використанням проросійськи налаштованих громадян України створюють тисячі фейкових аккаунтів з російським корінням для майбутнього втручання у виборчий процес. Тому в Україні існує необхідність у розробці та впровадженні дієвого механізму запобігання такому втручання.

**Результати аналізу наукових публікацій.** Інформаційна складова як один із факторів, який впливає на масову свідомість, докладно розглянута зарубіжними авторами, серед яких виділяються праці Г. Алмонда, Е. Вятра, Р. Даля, С. Верба, А. Вілдавскі, К. Дойча та ін.

Серед вітчизняних дослідників інформаційному протиборству приділяли увагу Бакалинський О.О., Гапеева О.Л., Горбулін В.П., Гулай В.В., Жарков Я.М., Мосов С.П., Нижник Н.Р., Остроухов В.В., Петрик В.М., Присяжнюк М.М. та ін.

Однак в науковій літературі відсутні системні дослідження, присвячені вивченню зарубіжного досвіду забезпечення інформаційної безпеки електоральних процесів.

**Метою статті** є аналіз зарубіжного досвіду у сфері забезпечення інформаційної безпеки електоральних процесів для його можливого запозичення та використання державними органами України.

**Виклад основного матеріалу.** Як зазначається у Доктрині інформаційної безпеки України, застосування РФ технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України. Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації [1]. Водночас, агресивна інформаційна війна здійснюється не тільки в Україні, а й на території інших країн світу.

У грудні 2016 року схвалено нову Доктрину інформаційної безпеки РФ, у положеннях якої чітко визначено, що головною метою дій РФ в інформаційній сфері визначається “прорив інформаційної блокади з боку США та ЄС” у рамках побудови “рівноправних міждержавних відносин в інформаційному просторі” та “формування вільного середовища обігу інформації”. У Доктрині відзначається відставання РФ від провідних західних країн у сферах комп’ютерних та телекомунікаційних технологій, що становить суттєву загрозу для Російської Федерації [4].

Невипадково протягом останнього часу відзначається надмірне посилення протиборства між країнами Заходу та РФ, перш за все, в інформаційній сфері, що пов’язано з активізацією спроб останньої здійснити вплив на політику США та ЄС у вигідному для себе напрямку. Найбільш резонансними проявами таких дій РФ стали спроби втручання в хід президентських виборів у США, а також у виборчі процеси окремих європейських країн, що викликає занепокоєння та негативну реакцію західних політичних кіл. Так, за результатами розслідувань дій Росії в ФРН, німецькі спецслужби

дійшли висновку щодо проведення російськими спецслужбами послідовної інформаційної політики з дестабілізації політичної обстановки в ФРН. Аналогічні дії російських спецслужб були відмічені спецслужбами Великої Британії, Франції, Австрії, Польщі та інших країн ЄС.

Розглянемо законодавчі ініціативи та практичні заходи, які вживаються євроспільнотою з метою протидії агресивній інформаційній експансії РФ та забезпечення власної інформаційної безпеки з урахуванням міжнародного досвіду забезпечення інформаційної безпеки електоральних процесів.

Після президентських виборів у США керівництвом Європейського Союзу було прийнято рішення щодо вироблення якісно нових підходів в інформаційному протиборстві з РФ. Так, у листопаді 2016 року Європейський Парламент ухвалив План імплементації нової Стратегії європейської політики безпеки і оборони, яка включає положення щодо протидії “гібридним” війнам та засобам “м’якої сили” з боку супротивників ЄС, у т.ч. в інформаційній сфері. Зазначене рішення було конкретизовано у резолюції Європейського Парламенту “Стратегічні комунікації ЄС, як протидія пропаганді третіх сторін”, яка була прийнята у листопаді 2016 року [5]. Ця резолюція вперше визнає застосування Росією агресивних методів з проведення ворожої пропаганди проти Європи, яка прирівнюється до загроз з боку терористичної організації “Ісламська держава”. У резолюції наголошується, що пропаганда РФ є частиною “гібридної війни”, яка спрямована на те, щоб “спотворити правду, посіяти сумніви і ворожнечу між країнами союзу, послабити стратегічну єдність ЄС і його північноамериканських партнерів, паралізувати процес прийняття рішення, дискредитувати інститут ЄС і трансатлантичне партнерство”.

Серед основних методів такої пропаганди РФ виділяють: розповсюдження неправдивої інформації в європейському інформаційному просторі, надання інформаційної та фінансової підтримки ультраправим, популістським та проросійським силам в країнах ЄС, а також позиціонування окремих регіонів Європи як “сфери традиційного впливу Російської Федерації”. Крім того, окремо відзначається використання РФ контактів з окремими європейськими партнерами з метою пропаганди та послаблення політичних позицій ЄС. За резолюцією головними організаторами інформаційних атак РФ є Міністерство закордонних справ РФ та Федеральне агентство “Россотрудничество”, які застосовують комплекс відповідних інструментів, включаючи засоби масової інформації, інформаційно-аналітичні центри та спеціальні фонди [5].

За оцінками європейських експертів, найбільшу загрозу для Європейського Союзу становлять російські псевдоновинні агентства та мультимедійні служби, зокрема: агентство Sputnik, телеканал RT (Russia Today) та фонд “Русский мир”. З урахуванням наведених обставин, у резолюції визначається перелік заходів з посилення протидії інформаційному впливу з боку Росії, зміст яких передбачає: розробку нової інформаційної стратегії ЄС; вивчення форм та методів дій РФ в інформаційній сфері; поглиблення взаємодії між європейськими інституціями з питань інформаційної безпеки; активізацію дій європейських ЗМІ у регіонах, які в найбільше зазнають впливу російської пропаганди; підвищення поінформованості європейської та світової спільноти щодо політики ЄС; підтримку незалежних засобів масової інформації в Росії; викриття злочинів колишніх комуністичних режимів в країнах Центрально-Східної Європи [6].

Для практичної реалізації наведених заходів планується нарощування можливостей “Оперативної групи по стратегічним комунікаціям на Сході” (East StratCom Task Force), яка створена у складі Європейської служби зовнішніх зв’язків (фактично – міністерство

закордонних справ Європейського Союзу), і опікується питаннями протидії інформаційному впливу з боку РФ. Сьогодні ця група фактично трансформувалася у повноцінне відомство зі збільшенням кількості співробітників, які працюють у напрямках Східної Європи, а також Північної Африки та Близького Сходу. Крім того, у грудні 2016 року між ЄС та НАТО було досягнуто домовленості щодо поглиблення взаємодії сторін у розвитку оборонного потенціалу, включаючи протидію “гібридним” війнам та посилення захисту кіберпростору. З цією метою планується створення “Європейського центру протидії гібридним загрозам” з широким спектром функцій, у т.ч. інформаційного протиборства. Окремим напрямом дій США, НАТО та ЄС є сприяння посиленню здатності їх партнерів протистояти інформаційній експансії з боку Росії, що, зокрема, передбачено комплексним планом допомоги Україні, який був прийнятий під час Варшавського саміту НАТО в липні 2016 року [7].

З метою систематизації та встановлення мінімальних вимог для всіх країн-членів ЄС у 2016 році була схвалена Директива Європейського Парламенту та Ради № 2016/1148 “Про загальні заходи безпеки мережевих та інформаційних систем”, положення якої зобов’язують уряди держав-членів визначати об’єкти критичної інфраструктури у різноманітних сферах [8]. Отже, з метою посилення кіберзахисту інформаційно-телекомунікаційних мереж та систем в ЄС були запроваджені Єдині нові правила. Виходячи із змісту вказаного документа, саме інформаційні мережі та системи відіграють життєво важливу роль в європейському суспільстві. Зважаючи на те, що глобальні мережі мають транснаціональний характер, істотні порушення штатного функціонування інформаційних систем цивільного або військового управління (незалежно від того, навмисні чи необережні ці дії) можуть негативно впливати на окремі держави-члени ЄС.

Причиною прийняття нової Директиви ЄС стала необхідність розробки дієвого механізму запобігання інцидентам у сфері інформаційної безпеки, що стосується обчислювальних мереж, серверів, систем зберігання даних і мережевих вузлів. Таким чином, ефективне реагування на вказані виклики безпеки мережевих та інформаційних систем вимагає глобального підходу на рівні ЄС, що охоплює загальне зміцнення технічного потенціалу, налагодження інформаційного обміну, співпраці і загальних вимог безпеки для операторів цифрових послуг. Ця Директива передбачає впровадження таких заходів щодо підвищення загального рівня кібербезпеки в ЄС, які забезпечать:

- відповідний рівень готовності держав-членів, що передбачає створення Команд швидкого реагування на кіберінциденти (Computer Security Response – CSIRT) і компетентних відповідальних національних органів;
- комплексну співпрацю між усіма державами-членами ЄС з метою надання підтримки та сприяння обміну інформацією між державами-членами про кіберзагрози та кіберінциденти;
- високий рівень безпеки у всіх секторах, які мають життєво важливе значення для економіки і суспільства, і крім того, значною мірою залежать від інформаційно-комунікаційних технологій (ІКТ), таких як: енергетика, транспорт, водопостачання, банківська сфера, інфраструктури фінансового ринку, охорони здоров’я та цифрової інфраструктури [8].

Окрім того, ключові постачальники цифрових послуг (пошукові системи, хмарні обчислення і он-лайніві торговельні майданчики) повинні відповідати вимогам безпеки і повідомляти про будь-які кіберінциденти. Також з метою досягнення високого рівня безпеки мережевих та інформаційних систем кожна країна ЄС зобов’язана розробити

Національні стратегії з безпеки мережевих та інформаційних систем, що визначають цілі і конкретні заходи, які повинні бути реалізовані.

У процесі здійснення імплементації положень цієї Директиви у серпні 2017 року декілька федеральних земель Німеччини звернулися до керівництва держави з проханням запровадити правила, які б зобов'язували соціальні мережі, зокрема "Facebook", надавати на вимогу правоохоронців конфіденційну інформацію про користувачів, оскільки влада федеральних земель обурюється тим, що керівництво "Facebook" залишає без відповіді в середньому 2/3 таких запитів: протягом останніх років поліція, прокуратура і спецслужби Німеччини відправляють на адресу "Facebook" щодня більше десяти запитів про надання особистих даних користувачів, зокрема про їх облікові дані або IP-адреси. Крім того, на вимогу правоохоронців має бути максимально скорочений термін надання таких облікових даних або інформації про користувачів [9].

Проте, ситуація кардинально змінюється.

У травні 2016 року Європейський Парламент і Рада затвердили постанову про нові правила і порядок захисту персональних даних ("Пакет захисту даних" ЄС), який передбачає створення умов забезпечення узгодженої нормативно-правової бази на європейському рівні та для всіх країн світу, які мають відносини з державами-країнами ЄС. "Пакет захисту даних" ЄС набув чинності 25 травня 2018 року та складається з трьох документів, головним з яких є Загальний регламент захисту даних (GDPR – General Data Protection Regulation) [10].

GDPR стосується будь-якої обробки персональних даних, зокрема їх збору, зберігання і передачі. За недотримання вимог GDPR компаніям загрожує втрата європейських клієнтів і ринків, а також штрафи до 20 млн євро або 2 – 4 % від річного фінансового обігу порушника. З огляду на глобальний характер Інтернету, GDPR встановлює стандарт конфіденційності даних у всьому світі, а його дія поширюється практично всі великі Інтернет-компанії, включаючи "Google", "Facebook", "Twitter" та ін.

Один із великих світових провайдерів мережа "Facebook" на початку 2018 року прозвітував, що контролює фейкові записи, у зв'язку з чим удосконалила свої системи розпізнавання та видалення недостовірних записів та фейкових новин. Компанія "Twitter" може почати повідомляти користувачам, чи піддавалися вони впливу контенту, згенерованого російським сервісом для поширення пропаганди. Соціальна мережа працює, щоб ідентифікувати й особисто поінформувати її користувачів, які побачили під час президентської компанії 2016 року твіти акаунтів, пов'язаних із прокремлівським "Агентством Інтернет-досліджень". "Twitter" виявила 1062 аккаунта, пов'язаних з російським "Агентством Інтернет-досліджень", відомим також як "фабрика тролів".

У вересні 2018 р. Конгрес США ухвалив Закон "Про кіберстримування та відповідні заходи", відповідно до положень якого офіційний Вашингтон має право запроваджувати санкції проти осіб, закордонних держав чи організацій, винних у вчиненні кіберзлочинів проти США [10]. На думку авторів закону, такий захід зможе захистити вибори та важливі об'єкти інфраструктури від "фінансованих іноземними державами навмисних кібератак", а також створить основу стримування та реагування на кібератаки проти США в майбутньому. Новий закон зобов'язує президента формувати списки небезпечних осіб, які загрожують "національній безпеці, закордонним справам, економічному розвитку чи фінансовій стабільності країни" [11].

Також практично одногласно ухвалено резолюцію про підтримку протидії російській пропаганді на рівні ЄС. Резолюція рекомендує країнам-членам ЄС заснувати органи (observatories) для відстежування дезінформації та фейків. У резолюції йдеться, що у деяких випадках державні засоби масової інформації були перетворені на



пропагандистські інструменти та використані для передачі фальшивих новин або розпалювання ненависті та ксенофобії проти меншин та певних груп. Це призводить до відсутності незалежності та низьких етичних стандартів у ряді засобів масової інформації та пояснює дедалі більшу недовіру населення. У зв'язку з цим Асамблея підтверджує свою підтримку рішення ПАРЄ від 2015 року про боротьбу з дезінформацією, яка походить із джерел ЗМІ та он-лайн-аккаунтів РФ, шляхом створення “Спеціальної групи East StratCom” [12].

Прояви російської інформаційної агресії також фіксує й політичне керівництво Франції, у зв'язку з чим у цій країні підготовлено проект закону для протидії фейкам на виборах. Минулорічна президентська кампанія у Франції ознаменувалася втручанням російських мас-медіа, кібератаками та загалом була визнана “брудною” за французькими стандартами. Враховуючи масштаби загроз в інформаційній сфері, у положеннях “Стратегічного огляду” (*Revue stratégique*) задекларовано, що питання дезінформації та її впливу стають одними з безпекових пріоритетів Франції [13].

Також у Франції на законодавчому рівні посилено заходи з контролю мас-медіа – для захисту країни від фальшивих новин – усі медіа, соцмережі, пошуковики, інформаційні портали матимуть певні зобов'язання стосовно “спонсорського контенту”, який вони розміщують. Також очікується збільшення повноважень Вищої наглядової ради радіотелебачення (*Conseil supérieur de l'audiovisuel, CSA*) для “боротьби зі спробами дестабілізації телеслужбами, що знаходяться під впливом іноземних держав”. Також з метою опору централізованій російській пропаганді у Франції законодавчо запроваджується право державного регулятора анулювати ліцензії телеканалів. Це стосується також й блокування контенту в соціальних мережах, що стане додатковим потужним інструментом з протидії російському впливу [14].

Не відстає від Франції й Німеччина, де також нещодавно було прийнято закон про боротьбу з фейковими новинами і з ненависницькими коментарями в соцмережах. Федеральне управління кримінальної поліції Німеччини (ВКА) повідомило про те, що в десяти німецьких землях, в тому числі в Берліні, Баварії, Гессені, Північному Рейні-Вестфалії, Саксонії, поліція провела операцію проти осіб, яких підозрюють у публікації в Інтернеті коментарів, що виражають ненависть. Поліція провела обшуки в квартирах підозрюваних, їх було допитано за висунутими звинуваченнями. Ці заходи торкнулися 29 осіб, яких звинувачують у публічних закликах до здійснення правопорушень, ксенофобських і антисемітських висловлювань. Обшуки стали частиною заходів по боротьбі з коментарями, що містять вказані висловлювання. За даними німецької поліції, в минулому році було зареєстровано 2,3 тис. таких висловлювань [15]. Наприкінці минулого року в Німеччині набув чинності закон, метою якого є боротьба з фейковими новинами та ненависницькими коментарями в соцмережах. Відповідно до цього закону, такі висловлювання повинні бути максимально швидко видалені з соцмереж, а їх авторам може загрожувати до 5 років позбавлення волі [15].

Також євроспільнота постійно шукає ефективні механізми протидії російській інформаційній експансії, зокрема поширенню фейкових новин. Так, наприкінці 2018 року у Брюсселі розпочала роботу група експертів, що протидіятиме поширенню неправдивої фейкової інформації у електронних ЗМІ. Ця комісія має розробити механізми розпізнавання фальшивих даних та запровадити обмеження щодо їх поширення. Перше завдання групи – дати визначення поняттю “фейкові новини” та підготувати пропозиції для подальших дій Єврокомісії. Група складається з 40 експертів, серед яких присутні фахівці із соціальних мереж, працівники ЗМІ, активісти, представники громадськості та провідні вчені [16].

Таким чином, світ вступає у нову виборчу фазу з урахуванням оновлень європейських інституцій. Сьогодні країни ЄС та США визнають глобальні масштаби російської агресивної інформаційної кампанії та вбачають в ній глобальну загрозу для їхнього інформаційного простору. У зв'язку з цим розроблюються нові законодавчі акти та впроваджуються практичні заходи, спрямовані на її суцільну нейтралізацію.

З урахуванням викладеного, саме результати активної фази протистояння між Заходом та РФ в інформаційній сфері визначатимуть розвиток ситуації в світі, яка безпосередньо впливає на Україну.

### **Висновки.**

Враховуючи масштаби російської інформаційної експансії та загрозливі тенденції у цій площині напередодні президентських та парламентських виборів у 2019 році в Україні, першочерговим завданням держави є системна боротьба з фейковими аккаунтами та російською пропагандою у вітчизняному інформаційному просторі.

З метою реалізації цього завдання доцільним вбачається вжиття заходів щодо:

- виявлення та припинення деструктивних дій окремих державних та неурядових структур суміжних країн: РФ, Румунії, Угорщини, Республіки Польщі, мінімізувати іноземний вплив та нейтралізувати їх наміри, які можуть негативно вплинути на шкоду національним інтересам України;
- виявлення, запобігання та припинення спроб представників політичних і релігійних об'єднань (насамперед, проросійських) політизувати та радикалізувати свою діяльність за підтримки закордонних центрів, інспірувати сепаратистські настрої та прояви релігійної ворожнечі серед етнічних громад, у тому числі й з використанням соціальних мереж, що може спричинити дестабілізацію суспільно-політичної обстановки, особливо у регіонах;
- виявлення і недопущення використання закордонними неурядовими організаціями та їх функціонерами можливостей вітчизняних ЗМІ, ресурсів мережі Інтернет, представників мас-медійних громадських організацій та інших фахових об'єднань для створення механізмів впливу, у т.ч. фінансових, на вітчизняну інформаційну сферу, суспільно-політичні процеси, здійснення дискредитації діяльності органів державної влади, а також проведення антиукраїнських інформаційних акцій, особливо напередодні виборів 2019 року.

### **Використана література**

1. Доктрина інформаційної безпеки України: Указ Президента України від 25.02.17 р. № 47. *Офіційний Вісник України*. 2017. № 20. Ст. 554.
2. Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки: Закон України від 09.01.07 р. № 537-V. *Офіційний Вісник України*. 2007. № 8. Ст. 273.
3. Кремль використовує всі можливі варіанти, щоб повернути Україну в свою сферу впливу. URL: <https://ru.tsn.ua/ukrayina/pyat-sposobov-kak-rossiya-mozhet-povliyat-na-ukrainskie-vybory-atlantic-council-1173792> (дата звернення: 20.12.2018).
4. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.16 г. № 646. URL: <https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html> (дата звернення: 20.12.2018).
5. Варшавський саміт НАТО і російська загроза. URL: [https://www.bbc.com/ukrainian/politics/2016/07/160708\\_warsaw\\_nato\\_summit\\_ozh](https://www.bbc.com/ukrainian/politics/2016/07/160708_warsaw_nato_summit_ozh) (дата звернення: 17.01.2019).
6. Нові аспекти інформаційного протистояння між Росією та Заходом. URL: <http://bintel.com.ua/uk/article/02-18-infowar> (дата звернення: 17.01.2019).
7. Про загальні заходи безпеки мережевих та інформаційних систем: Директива Європейського Парламенту та Ради № 2016/1148. URL: [https://zakon.rada.gov.ua/laws/show/994\\_242/card5](https://zakon.rada.gov.ua/laws/show/994_242/card5) (дата звернення: 17.01.2019).

8. Стосовно заходів щодо забезпечення високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі: Директива Європейського Парламенту та Ради від 6 липня 2016 р. № 2016/1148. URL: <http://eur-lex.europa.eu/eli/dir/2016/1148/oj> (дата звернення: 20.12.2018).

9. У Німеччині пропонують соцмережі зобов'язати до співпраці зі спецслужбами URL: <http://www.eurointegration.com.ua/news/2016/08/7/7053101> 9 (дата звернення: 20.12.2018).

10. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних: збірник перекладу документів ("Пакет захисту даних" Європейського Парламенту і Ради від 2016 р.) пер. з англ. І. Майстренко / за ред. В. Брижко; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). Київ: ТОВ "Видавничий дім "АртЕк", 2018. 180 с.

Регламент (ЄС) 2016/679 від 27 квітня 2016 р. (General Data Protection Regulation). URL: <https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-2016679.pdf> (дата звернення: 17.01.2019).

11. У США схвалили закон про запровадження санкцій за кібератаки. URL: [https://24tv.ua/u\\_ssha\\_shvalili\\_zakon\\_pro\\_zaprovadzhennya\\_sanktsiy\\_pro\\_kiberataki\\_n1027167](https://24tv.ua/u_ssha_shvalili_zakon_pro_zaprovadzhennya_sanktsiy_pro_kiberataki_n1027167) (дата звернення: 17.01.2019).

12. ПАРЄ прийняла резолюцію щодо протидії пропаганді РФ. URL: <https://uatv.ua/parye-prujnyala-rezolyutsiyu-shhodo-protydyi-propagandi-rf> (дата звернення: 17.01.2019).

13. Стратегічний огляд (Revue stratégique) URL: <https://www.defense.gouv.fr/dgris/presentation/evenements/revue-strategique-de-defense-et-de-securite-nationale-2017> (дата звернення: 28.12.2018).

14. Якщо поглянути на Францію, то вона готує новий закон для протидії фейкам на виборах. Пропаганду забанять у Google. URL: <https://www.eurointegration.com.ua/articles/2018/03/20/7079007> (дата звернення: 28.12.2018).

15. У Німеччині прийшли з обшуками до тих, хто пише ксенофобські коментарі в Інтернеті. URL: <https://mind.ua/news/20185840-u-nimechchini-prijshli-z-obshukami-do-tih-hto-pishe-ksenofobski-komentari-v-interneti> (дата звернення: 17.01.2019).

16. Соціальні мережі як чинник інформаційної безпеки. Огляд Інтернет-ресурсів (01. – 16.01.2018). URL: <http://www.nbuviap.gov.ua/images/sozinfo/2018/1.pdf> (дата звернення: 28.12.2018).

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

УДК 343.2/.7:004.056(477)

ГАВЛОВСЬКИЙ В.Д., кандидат юридичних наук, старший науковий співробітник, головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України

АНАЛІЗ СТАНУ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Анотація. В статті досліджуються питання, що виникають при формуванні статистичної звітності із протидії кіберзлочинності в Україні. Надано порівняльний аналіз стану кіберзлочинності за 2018 р.

Ключові слова: кіберзлочинність, аналіз стану кіберзлочинності, статистичні звітності.

Summary. The article examines the issues that arise when forming statistical reporting on combating cybercrime in Ukraine. The comparative analysis of the state of cybercrime for 2018 is presented.

Keywords: cybercrime, analysis of the state of cybercrime, statistical reporting.

Аннотация. В статье исследуются вопросы, возникающие при формировании статистической отчетности по противодействию киберпреступности в Украине. Предоставлено сравнительный анализ киберпреступности за 2018 год.

Ключевые слова: киберпреступность, анализ киберпреступности, статистические отчетности.

Постановка проблеми. У засобах масової інформації, Інтернеті викладається величезний обсяг інформації про вчинені кіберзлочини, збитки від них, про потерпілих, окремі аналізи кіберзлочинності в межах однієї країни або групи країн тощо. Але сьогодні, на думку фахівців, жоден комплексний кримінологічний аналіз не здатний скласти повного уявлення про глобальні масштаби кіберзлочинності.

Насамперед, це явище за своєю природою транскордонне. Глобальність і транскордонність комп'ютерних і телекомунікаційних мереж, можливість маніпуляцій з ідентичністю створює ситуації, коли злочинець, перебуваючи на одному континенті, вчиняє злочин на другому, а наслідки злочину настають на третьому. І всі події відбуваються в кіберпросторі. А втім, національне кримінальне законодавство у сфері боротьби з кіберзлочинністю, практика його застосування, підходи до формування кримінальної статистики в країнах різні. Кримінологічні дослідження, як правило, спираються на дані облікованої злочинності, не заглиблюючись у соціальні, економічні, політичні, демографічні, організаційні та інші причини кіберзлочинності.

Окремі аспекти аналізу злочинності, зокрема кіберзлочинності, вивчали О.М. Бандурка, В.В. Василевич, В.В. Голіна, Б.М. Головкін, А. П. Закалюк, О.М. Литвинов, В.В. Марков, В.І. Трапезніков, В.О. Туляков та багато ін. вчених (див., зокрема, [1 – 4]). Разом з тим, проблемним питанням, які виникають при аналізі злочинності, зокрема статистичної звітності, приділяється недостатньо уваги.

Виклад основного матеріалу. В Україні відсутня офіційна державна статистика, яка б містила відомості про кіберзлочини, що негативно позначається на запобіжних заходах, які мають фрагментарний характер, зумовлюючи труднощі у протидії та боротьбі з таким видом суспільно небезпечних діянь.

Серед причин зазначеного, зокрема, те, що терміном “кіберзлочинність” (визначений лише 2017 р. у Законі України “Про основні засади забезпечення кібербезпеки України” [5]) охоплюється широкий спектр правопорушень, ускладнюючи тим самим розробку системи типології або класифікації кіберзлочинності.

Під поняттям “кіберзлочини” ми розуміємо кримінальні правопорушення, передбачені розділом XVI КК України (“Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів, систем та комп’ютерних мереж і мереж електрозв’язку”), та зареєстровані кримінальні провадження із кваліфікуючою відміткою в картці про кримінальне правопорушення – “з використанням високих інформаційних технологій і телекомунікаційних мереж”.

На сьогодні офіційна державна статистика містить лише відомості про вчинені кримінальні правопорушення, передбачені Розд. XVI КК України, що відображаються у звітах Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення; Єдиний звіт про осіб, які вчинили кримінальні правопорушення).

У Державній судовій адміністрації України готуються звіти судів першої інстанції про розгляд матеріалів кримінального провадження (форма № 1-к), про осіб, притягнутих до кримінальної відповідальності, та види кримінального покарання (форма № 6) і про склад засуджених (форма № 7).

Варто визначити, що до 2018 р. склалися піврічні й річні звіти. Але з метою вдосконалення звітності про стан здійснення правосуддя місцевими та апеляційними судами Державною судовою адміністрацією України видано наказ “Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами” від 23 червня 2018 р. № 325 [6]. Зараз періодичність цих звітів річна. Термін підготовки і подання звітів Державною судовою адміністрацією України до Державної служби статистики України – не пізніше 40-го дня після звітного періоду (для порівняння – Генеральна прокуратура України подає звіти до Державної служби статистики України до 5 числа після звітного періоду).

Статистичні дані про кіберзлочини відображаються також у відомчій статистичній звітності Національної поліції України, зокрема у Звіті про результати роботи підрозділів Національної поліції України, де, крім кримінальних правопорушень, охоплених Розд. XVI КК України, зазначається ще низка кримінальних правопорушень, що вчинені з використанням електронно-обчислювальної техніки, передбачених ст. 176 КК України “Порушення авторського права і суміжних прав” і ст. 185 КК України “Крадіжка”, чч. 3 і 4 ст. 190 КК України “Шахрайство”, ст. 200 КК України “Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення”, ст. 229 КК України “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 КК України “Ввезення, виготовлення, збут і розповсюдження порнографічних предметів”. Але цей перелік статей неповний.

Варто відмітити, що зважаючи на високий рівень латентності кіберзлочинності (наразі обліковується тільки 10 – 20 % вчинених злочинів, а решту становить латентна злочинність), а також низький рівень звітно-реєстраційної дисципліни, сьогодні говорити про будь-яку офіційну статистику, яка повно й достовірно відображає стан і структуру кіберзлочинності, проблематично. Можливо проаналізувати тільки динаміку

цього виду злочинності, структуру злочинності, стан криміногенної ситуації у цій сфері на основі облікованих злочинів.

Протягом 2018 р., згідно зі статистичними даними Генеральної прокуратури України (див. Табл. 1), обліковано 2017 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Їх питома вага ще незначна і становить усього 0,5 % від усіх облікованих кримінальних правопорушень у 2018 р., але за останні п'ять років зростає в 5,6 раза (у 2014 р. становила – 0,09 %).

Таблиця 1. Обліковані кримінальні правопорушення, передбачені статтями Розд. XVI КК України (за даними Генеральної прокуратури України)

| Статті
КК України | 2017 р. | 2018 р. | У порівнянні 2017 і 2018 рр. | |
|----------------------|---------|---------|------------------------------|---------|
| | | | +/- | % |
| 361 | 1795 | 1023 | -772 | -43,0 % |
| 361 ¹ | 35 | 134 | 99 | 282,9 % |
| 361 ² | 64 | 52 | -12 | -18,8 % |
| 362 | 670 | 1070 | 400 | 59,7 % |
| 363 | 6 | 12 | 6 | 100,0 % |
| 363 ¹ | 3 | 10 | 7 | 233,3 % |
| Усього | 2573 | 2301 | -272 | -10,6 % |

Порівняно із 2017 р. кількість кримінальних правопорушень, передбачених статтями Розд. XVI КК України, зменшилася на 10,6 % (у 2017 р. – 2573). При цьому кількість кримінальних правопорушень, за якими особам вручено повідомлення про підозру, збільшилася на 26,4 % (1272 у 2017 р. проти 1608 у 2018 р.), зокрема передбачених ст. 362 КК України “Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї”, на 58,2 % (607 у 2017 р. проти 960 у 2018 р.).

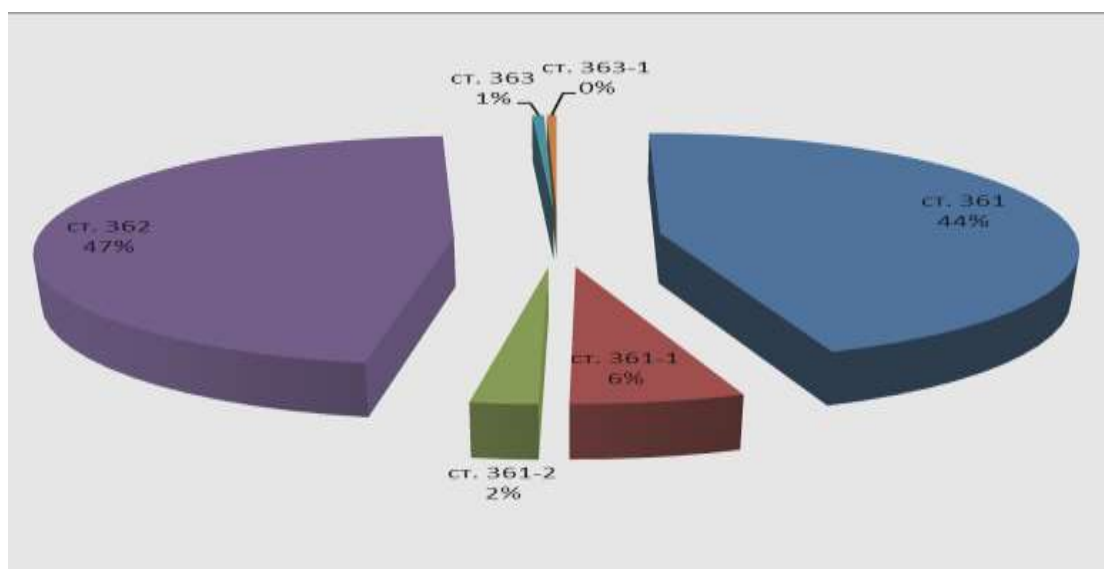
Також збільшилася кількість кримінальних правопорушень, за якими провадження направлено до суду з обвинувальним актом, – на 31,0 % (1015 у 2017 р. проти 1220 у 2018 р.).

Спостерігається незначне (на 1,3 %) зменшення кількості тяжких кримінальних правопорушень – 1591 у 2017 р. проти 1270 у 2018 р.

Збільшилася кількість майже всіх кримінальних правопорушень цієї категорії, крім передбачених ст. 361 КК України “Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку”, чисельність яких зменшилася на 772 кримінальні правопорушення, завдяки чому зменшилася кількість кримінальних правопорушень, передбачених статтями Розд. XVI КК України.

Водночас кількість кримінальних правопорушень, передбачених розділом XVI КК України, що вчинені групою осіб, за якими провадження направлено до суду, зростає на 4,8 % (42 у 2017 р. проти 44 у 2018 р.).

На 45,9 % (142 у 2017 р. проти 771 у 2018 р.) зменшилася чисельність кримінальних правопорушень, щодо яких наприкінці 2018 р. рішення не прийнято (про закінчення або припинення).



Мал. 1. Питома вага кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку

Як видно з Мал. 1, найбільшу частку правопорушень в зазначеній сфері становлять кримінальні правопорушення, передбачені ст. 362 КК України (47 %) та ст. 361 КК України (44 %).

Таблиця 2. Обліковані у 2018 р. кримінальні правопорушення, передбачені статтями Розд. XVI КК України та ст. 362 КК України з наростаючим підсумком та помісячно

| Розділ XVI | січ. | лют. | бер. | квіт. | трав. | черв. | лип. | серп. | вер. | жовт. | лист. | груд. |
|-------------------------|------|------|------|-------|-------|-------|------|-------|------|-------|-------|-------|
| з наростаючим підсумком | 272 | 597 | 982 | 1275 | 1487 | 1637 | 1726 | 1885 | 2017 | 2130 | 2245 | 2301 |
| щомісячно | 272 | 325 | 385 | 293 | 212 | 150 | 89 | 159 | 132 | 113 | 115 | 56 |

| ст. 362 | січ. | лют. | бер. | квіт. | трав. | черв. | лип. | серп. | вер. | жовт. | лист. | груд. |
|-------------------------|------|------|------|-------|-------|-------|------|-------|------|-------|-------|-------|
| з наростаючим підсумком | 190 | 363 | 564 | 700 | 780 | 806 | 836 | 909 | 951 | 1027 | 1062 | 1070 |
| щомісячно | 190 | 173 | 201 | 136 | 80 | 26 | 30 | 73 | 42 | 76 | 35 | 8 |

Із Табл. 2 прослідковується, що найбільшу кількість кримінальних правопорушень було обліковано в березні – 385, найменшу – в грудні – 56, що майже в 7 разів менше. При цьому кримінальних правопорушень, передбачених ст. 362 КК України у грудні, обліковано у 25 разів менше порівняно з березнем (8 у грудні проти 201 у березні).

Варто відзначити, що у січні 2019 року обліковано 218 кримінальних правопорушень, передбачених статтями Розд. XVI КК України, а передбачених ст. 362 КК України – 90. На час вчинення кримінального правопорушення 45 осіб були у віці від 18 до 28 років, 47 – від 29 до 39 років, 22 – від 40 до 54 років, 15 – 60 і більше років. Таким чином, за віковою ознакою неможливо виокремити якусь явну категорію правопорушників. Виявлено 42 жінки (30,9 %), що вчинили кримінальні правопорушення, тобто третина виявлених правопорушників – жінки. За освітою на час вчинення кримінального правопорушення найбільшу кількість становили особи з повною вищою і базовою вищою освітою – 77

(56,6 %), з професійно-технічною – 27 осіб, з повною загальною середньою та базовою загальною середньою освітою – 31 особа.

Із 136 виявлених осіб, які вчинили правопорушення, передбачені Розд. XVI КК України, всі є громадянами України, майже половина осіб є працездатними, які не працювали і не навчалися, – 46 та 21 – безробітні, 8 учнів і студентів навчальних закладів.

Групою осіб у 2018 році у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку вчинено 44 кримінальних правопорушення, що становить 3,3 % від облікованих і на 4,8% більше порівняно з 2017 роком.

Найбільше групою осіб вчинено кримінальних правопорушень, передбачених ст. 361 КК України, – 37.

Розглянемо судову статистику. У судах першої інстанції у 2018 році перебували на розгляді 198 проваджень (справ) за статтями Розд. XVI КК України, з них 135 надійшли протягом року, що на 70,9 % більше у порівнянні з 2017 роком (надійшло 79).

У 2018 році розглянуто 96 проваджень, що майже у два рази більше ніж у 2017 році (50). З них 63 – із постановленням вироку, 23 із закриттям провадження у справі, 5 – повернуто прокурору. На кінець 2018 року залишилося 102 нерозглянутих провадження, що на 64,5 % більше у порівнянні з 2017 роком (62).

Кількість осіб, провадження щодо яких перебували в суді, складала 224, що на 57,7 % більше у порівнянні з 2017 роком (142). Кількість осіб, судові рішення щодо яких набрали законної сили складає 70 (у 2017 році – 56), з них 49 осіб засуджено (70 %), 28,6 % (20) складають особи, матеріали кримінального провадження у відношенні яких закрито. Призначено покарання у вигляді позбавлення волі на певний строк 3 особам (у 2017 році – 7), 23 особи оштрафовано, 20 осіб звільнено від покарання з випробувальним строком і 3 унаслідок амністії. За сукупністю злочинів призначено покарання 15 особам. Найбільше засуджено осіб за статтею 361 КК України – 26.

Варто вказати, що лише 4,3 % (3 з 70 осіб) становлять особи, яких позбавили волі на певний строк: понад 2 роки до 3 років включно – 1 і понад 3 років до 5 років включно – 2.

Також слід відзначити, що всі із 49 засуджених осіб є громадянами України, кожен п'ятий із засуджених – жінки (10). Найбільше засуджених – це особи в віці від 30 до 50 років – 18 (36,7 %), від 18 до 25 років – 30,6 % (15), від 25 до 30 років – 22,4 % (11).

Більш повний аналіз стану кіберзлочинності можна зробити, використавши відомчу звітність Національної поліції України, зокрема Звіт про результати роботи підрозділів Національної поліції України за 2018 р.

Аналізуючи дані статистичних звітів, слід звертати увагу на можливі розбіжності між ідентичними показниками різних звітів.

Як приклад, відповідно до статистичного звіту Генеральної прокуратури України (Єдиний звіт про кримінальні правопорушення – Розд. 4, Табл. 4.15), у 2018 р., обліковано 2241 кримінальне правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (Розд. XVI КК України), а у відомчому звіті Національної поліції України кількість вчинених кримінальних правопорушень, передбачених статтями Розд. XVI КК України, становить 2374 (різниця – 133). При цьому, відповідно до звітності Генеральної прокуратури України, зменшення кількості облікованих кримінальних правопорушень порівняно з 2017 роком складає 10,94 %, а відповідно до звітності Національної поліції України – 2,9 %.

Також, зокрема за статистичним звітом Генеральної прокуратури України, обліковано 1007 кримінальних правопорушень, передбачених ст. 361 КК України, а у відомчому звіті Національної поліції України кількість вчинених кримінальних правопорушень, передбачених цією статтею, за цей же період становить 1108 (різниця – 101 кримінальне правопорушення).

З порівняльного аналізу злочинів, учинених із використанням високих інформаційних технологій (за даними Національної поліції України), випливає, що кількість кримінальних правопорушень, вчинених у 2018 р., зменшилася на 14,0 % порівняно з 2017 р. (6974 у 2017 р. проти 6001 у 2018 р.). При цьому, варто зазначити, що на 22,4 % збільшилася кількість кримінальних правопорушень, досудове розслідування за якими не закінчено: з 4930 у 2017 р. до 6035 у 2018 р.

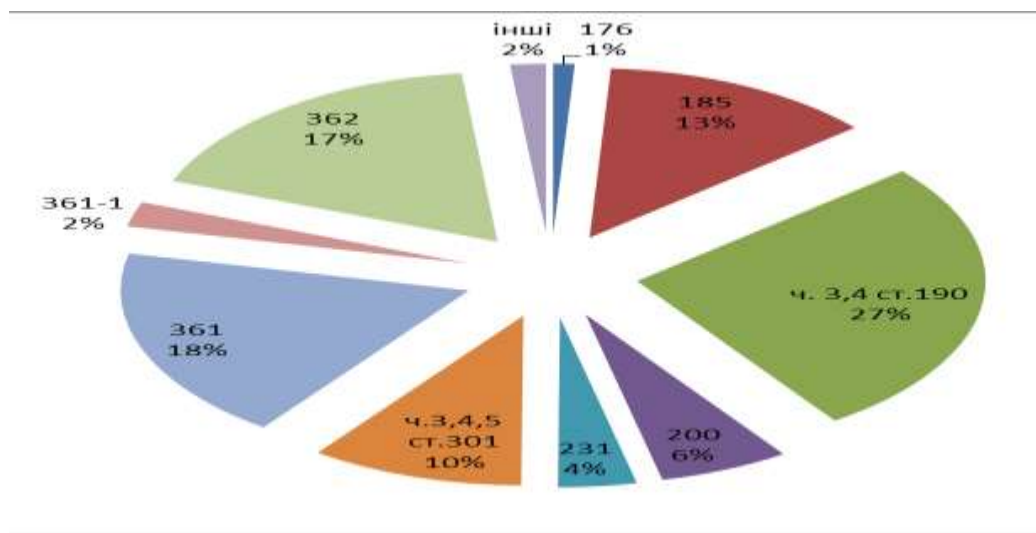
Аналіз динаміки даного виду злочинності свідчить про те, що відбулося різке зниження кількості злочинів, передбачених чч. 3 і 4 ст. 190 КК України, – на 1200 (42,9 %) (2798 у 2017 р. проти 1598 у 2018 р.). На 10,8 % зменшилася чисельність крадіжок, вчинених із використанням електронно-обчислювальної техніки (860 у 2017 р. проти 767 у 2018 р.).

Слід звернути увагу на значне (у 3,8 раза) збільшення кількості кримінальних правопорушень, передбачених ст. 231 КК України, – на 275,9 % (58 у 2017 р. проти 218 у 2018 р.). На 28,9 % збільшилася кількість злочинів, передбачених чч. 3, 4 і 5 ст. 301 КК України (463 у 2017 р. проти 597 у 2018 р.). У 2 рази зросла чисельність злочинів, передбачених ст. 176 КК України (29 у 2017 р. проти 59 у 2018 р.).

Таблиця 3. Обліковані кримінальні правопорушення, вчинені з використанням високих інформаційних технологій

| Статті
КК України | 2017 р. | 2018 р. | У порівнянні 2017 і 2018 рр. | |
|----------------------|---------|---------|------------------------------|---------|
| | | | +/- | % |
| 176 | 29 | 59 | 30 | 103,4 % |
| 185 | 860 | 767 | -93 | -10,8 % |
| чч. 3 і 4 ст. 190 | 2798 | 1598 | -1200 | -42,9 % |
| 200 | 311 | 364 | 53 | 17,0 % |
| 229 | 10 | 24 | 14 | 140,0 % |
| 231 | 58 | 218 | 160 | 275,9 % |
| чч. 3, 4 і 5 ст. 301 | 463 | 597 | 134 | 28,9 % |
| 361 | 1618 | 1108 | | |
| 361 ¹ | 28 | 142 | | |
| 361 ² | 57 | 49 | | |
| 362 | 729 | 1049 | | |
| 363 | 11 | 15 | | |
| 3631 | 2 | 11 | | |
| Розд. XVI | 2445 | 2374 | -71 | -2,9 % |
| Усього | 6974 | 6001 | -973 | -14,0 % |

В Україні серед злочинів, учинених із використанням високих інформаційних технологій у 2018 р., за даними Національної поліції, найбільшу питому вагу становлять кримінальні правопорушення, передбачені чч. 3 і 4 ст. 190 КК України – 27 %, ст. 361 КК України – 18 %, ст. 362 КК України – 17 %, чч. 3, 4 і 5 ст. 301 КК України – 10 % (див. Мал. 2).



Мал. 2. Питома вага кримінальних правопорушень, вчинених з використанням високих інформаційних технологій

Пропорційно зменшенню кількості правопорушень, вчинених із використанням високих інформаційних технологій, зменшилася й чисельність осіб, яким повідомлено про підозру у вчиненні кримінального правопорушення (980 у 2017 р. проти 803 у 2018 р.), що становить 18,1 %. Також на 12,8% зменшилася кількість осіб, яким пред'явлені обвинувальні акти: з 764 у 2017 р. до 666 у 2018 р.

Кіберзлочини вчиняють переважно індивідууми або невеликі злочинні групи хакерів.

Працівники підрозділів кіберполіції Національної поліції України порівняно з попереднім періодом виявили на 4 організовані групи і злочинні організації більше (7 у 2017 р. проти 11 у 2018 р.). Вони вчинили 142 кримінальних правопорушень, з яких 140 – тяжкі. Найбільше – передбачених ст. 190 ККУ України (100), у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (7).

У 2018 р. виявлено 196 фактів 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, що на 37,1 % більше порівняно з 2017 р. (143), і в 7,5 рази порівняно з 2016 р. (26).

При цьому, варто відзначити, що у ЗМІ ці показники подаються як кількість виявлених груп, які збували наркотичні засоби з використанням Інтернету [7].

У сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку організованими групами вчинено 9 кримінальних правопорушень: із них 6 – виявили працівники підрозділів кіберполіції, 3 – підрозділів захисту економіки.

Виявлено 41 особу, яка вчинила кримінальні правопорушення у складі ОГ і ЗО, що на 51,9 % більше порівняно з 2017 р. (27 осіб).

Слід зазначити, що у 2018 р. 72 кримінальних правопорушення у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку виявили працівники підрозділів карного розшуку (проти 163 у 2017 р.).

У 2018 р. кримінальними правопорушеннями, вчиненими з використанням високих інформаційних технологій, завдано матеріальних збитків на суму 38 713 тис. грн, що на 51 674 тис. грн менше, ніж у попередньому періоді (90387 тис. грн). При цьому у 2017 р. відшкодовано (з урахуванням накладеного арешту та вилученого майна) 71,8 % коштів, а у 2018 р. – лише 57,2 %. У 2018 р. найбільших матеріальних збитків завдано шахрайством – 21 194 тис. грн, при цьому відшкодовано лише 53,1 % (11 250 тис. грн).

У 2018 р. збільшення кількості кримінальних правопорушень, що вчинені з використанням високих інформаційних технологій, відзначалося у 8 областях. Найбільше зростання відбулося в Миколаївській (106,9%), Рівненській (93,5%), Харківській (85,5%) областях (див. Табл. 4).

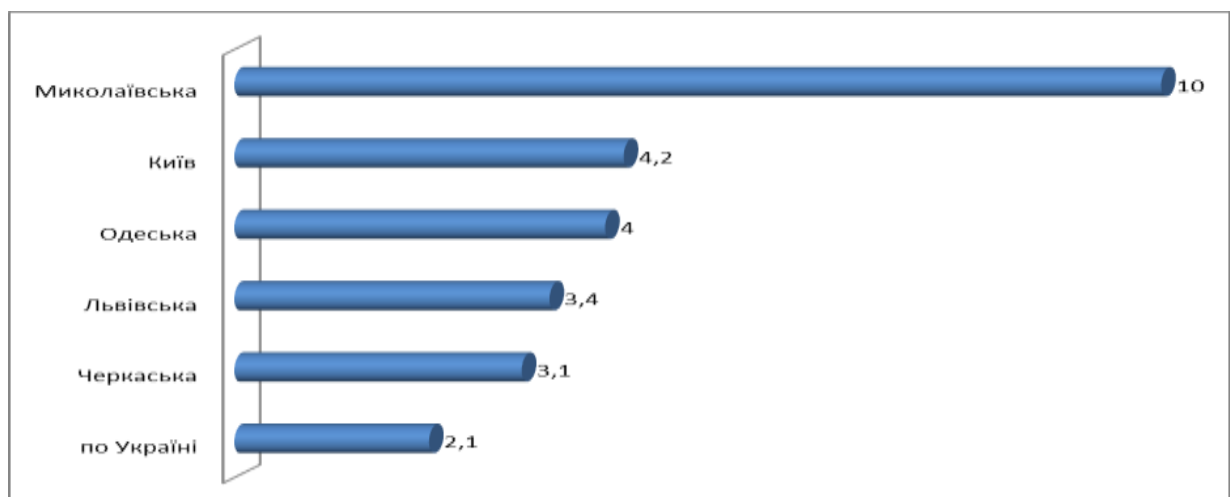
Таблиця 4. Найбільше зростання і найбільше зменшення кількості вчинених кримінальних правопорушень, вчинених з використанням високих інформаційних технологій

| | 2017 | 2018 | + /- | % |
|-------------------|------|------|------|---------|
| Миколаївська | 375 | 776 | 401 | 106,9 % |
| Рівненська | 77 | 149 | 72 | 93,5 % |
| Харківська | 117 | 217 | 100 | 85,5 % |
| Полтавська | 94 | 145 | 51 | 54,3 % |
| Вінницька | 122 | 149 | 27 | 22,1 % |
| Івано-Франківська | 235 | 122 | -113 | -48,1 % |
| Київська | 295 | 127 | -168 | -56,9 % |
| Чернівецька | 298 | 125 | -173 | -58,1 % |
| Волинська | 133 | 51 | -82 | -61,7 % |
| Кіровоградська | 252 | 94 | -158 | -62,7 % |

Найбільше кримінальних правопорушень вчинено в м. Києві (845), Миколаївській (776), Одеській (647) та Львівській (591) областях, найменше – у Волинській області (51).

Рівень кіберзлочинності в Україні на 10 000 населення невисокий і у 2018 р. складав 2,1 проти 2,4 у 2017 р. При підрахунку використовувалися показники Державної служби статистики України, зокрема статистичного збірника “Розподіл постійного населення України за статтю та віком (на 1 січня 2018 року)”. Вікова категорія населення складала 15 – 64 років.

У 5 областях України рівень злочинності на 10 000 населення вищий ніж загалом по Україні. Найвищий – у Миколаївській області – 10,0. Дещо нижчий – у м. Києві (4,2), Одеській (4,0), Львівській (3,4) та Черкаській областях. Найнижчий у Закарпатській, Волинській та Донецькій (3,1) областях менше 1 (див. Мал. 4).



Мал. 4. Рівень злочинності на 10000 населення

Найбільше злочинів, передбачених чч. 3 і 4 ст. 190 КК України, вчинено в Одеській (280), Дніпропетровській (191), Луганській (174), Харківській (149) областях; крадіжок із використанням електронно-обчислювальної техніки – в Миколаївській області (145), м. Києві (112), Дніпропетровській і Сумській областях (81 і 73 відповідно); передбачених чч. 3, 4 і 5 ст. 301 КК України – у м. Києві (299), Івано-Франківській (82) та Донецькій (55) областях; несанкціонованих втручань у роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, відповідальність за які передбачена ст. 361 КК України – в Одеській (141), Львівській (140), Миколаївській (126) областях; у Миколаївській області – злочинів, передбачених ст. 362 КК України – 241, в Одеській області – 207, в м. Києві – 125.

Варто звернути увагу на деякі особливості вчинення кримінальних правопорушень за регіонами.

Так, у Львівській області – 34 з 59 вчинених по Україні кримінальних правопорушень, передбачених ст. 176 КК України, що становить 57,6 %.

36,3 % кримінальних правопорушень, передбачених ст. 200 КК України, вчинено в м. Києві (132 із 364).

Кримінальні правопорушення, передбачені ст. 231 КК України, мали місце лише в Миколаївській (117) і Львівській (101) областях.

У м. Києві вчинено 50,1 % кримінальних правопорушень, передбачених ст. 301 КК України (299 із 597).

У Запорізькій області вчинено 8 із 11 кримінальних правопорушень, передбачених ст. 363 КК України.

Висновки.

Дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів.

Згадані вище звіти розроблені без врахування подальшого аналізу кіберзлочинності. І якщо у звіті Національної поліції України містяться дані про певну кількість злочинів, які можна віднести до кіберзлочинів, в офіційних статистичних звітах, крім Розділу XVI КК України, такі показники відсутні.

Тож, про офіційну статистику, яка повно й достовірно відображає стан і структуру кіберзлочинності, сьогодні говорити проблематично. Можливо проаналізувати тільки динаміку цього виду злочинності, структуру злочинності на основі облікованих злочинів.

Вказане може свідчити про необхідність визначення критеріїв щодо віднесення кримінальних правопорушень до категорії кіберзлочинів із подальшою розробкою статистичної звітності про зареєстровані кіберзлочини, про осіб, які їх вчинили, та результати боротьби з кіберзлочинністю.

Використана література

1. Кримінологічний довідник / О.М. Бандурка, В.С. Батиргарєєва, О.М. Литвинов та ін. / за наук. ред. О.М. Бандурки. Харків: Золота миля, 2013. 412 с.
2. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини: навч. посіб. Харків: Право, 2014. 513 с.
3. Марков В.В. Статистичне дослідження показників кіберзлочинності: методологічний аспект. *Право і Безпека*. 2013. № 2. С. 136-139.

4. Трапезников В.И. Характеристика и значение международной статистики киберпреступности. *Информатика та математичні методи в моделюванні*. 2014. Т. 4. № 4. С. 363–369.

5. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VII (База даних “Законодавство України” / ВР України). URL: <http://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 07.11.2018).

6. Про затвердження річних форм звітів щодо здійснення правосуддя місцевими та апеляційними судами: наказ Голови Державної судової адміністрації від 23.06.18 р. № 325. URL: https://dsa.court.gov.ua/dsa/inshe/14/№_325_18 (дата звернення: 07.11.2018).

7. В 2016 правоохоронители обнаружили 26 групп в Украине, которые сбывали наркотики через Интернет. В 2018 таких групп обнаружили 196. URL: https://censor.net.ua/news/3107598/za_2018_god_politsiya_raskryla_196_grupp_sbyvayuschih_narkotiki_cherez_internet_zamnachalnik_departamenta

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

УДК 343.9.024 : 004.056

**ГУЦАЛЮК М.В.,** доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.,  
провідний науковий співробітник Міжвідомчого науково-дослідного  
центру з проблем боротьби з організованою злочинністю  
при РНБО України

## СУЧАСНІ ТЕНДЕНЦІЇ ОРГАНІЗОВАНОЇ КІБЕРЗЛОЧИННОСТІ

**Анотація.** В статті досліджуються сучасні тенденції кіберзлочинності, зокрема організовані її форми. Пропонуються заходи щодо посилення протидії кіберзлочинності.

**Ключові слова:** кіберзлочинність, “Даркнет”, міжнародне співробітництво.

**Summary.** The article investigates the current trends of cybercrime, in particular, its organized forms. Measures to enhance the fight against cybercrime are proposed.

**Keywords:** cybercrime, “DarkNet”, international cooperation.

**Аннотация.** В статье исследуются современные тенденции киберпреступности, в частности, ее организованные формы.

**Ключевые слова:** киберпреступность, “Даркнет”, международное сотрудничество.

**Постановка проблеми.** Серед основних ознак сучасного інформаційного суспільства слід зазначити бурхливий розвиток інформаційних технологій та поширення мережі Інтернет, які впроваджуються у всі сфери життєдіяльності. Якщо перший в історії веб-сайт було створено в 1991 році, то на сьогодні у світі існує вже понад 1,3 мільярда веб-сайтів. Постійно зростає кількість Інтернет-користувачів: у 1995 році було лише 16 млн, у 2005 – 1 млрд, а у 2018 році – понад 4 млрд [1]. В Україні, за результатами дослідження агентства “PlusOne”, кількість користувачів соціальної мережі Facebook за останні 5 років зросла на 9,8 млн (+ 306,2 %) і нині становить 13 млн. [2].

Використання кіберпростору сприяє обміну інформацією по всьому світу та забезпечує свободу вираження поглядів. Соціальні мережі принципово змінили методи взаємодії людей, а штучний інтелект та хмарні обчислення нині дозволяють обробляти значні обсяги даних та впроваджувати різноманітні новації, які сприяють становленню якісно нового рівня розвитку людини, держави та суспільства.

Водночас з’явилася і новітня форма злочинної діяльності – кіберзлочинність, яка сьогодні опанувала середовище комп’ютерних мереж і мобільних пристроїв. Анонімність глобальних інформаційних мереж та швидкість передачі інформації дає змогу використовувати ці переваги не тільки для розвитку інформаційного суспільства, але й для вчинення протиправних діянь. Цьому сприяє і те, що інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть на це реагувати. Тому злочинність у кіберпросторі – одна з найгостріших проблем, яка постала сьогодні перед міжнародним співтовариством.

Генеральний секретар Організації Об’єднаних Націй Антоніу Гутерріш у травні 2018 року у день відкриття 27-ї сесії Комісії ООН з попередження злочинності та кримінального правосуддя зазначив, що нові технології, включаючи великі дані і аналітику, штучний інтелект та автоматизацію надають значні переваги для людства, але, разом з тим, створюють нові форми злочинності. Збитки світової економіки від кіберзлочинності оцінюються у \$ 1,5 трлн. на рік. А за негативним сценарієм у 2019 році вони сягатимуть \$ 2 трлн. [3].

**Результати аналізу наукових публікацій.** Різні аспекти проблем боротьби з кіберзлочинністю були предметом дослідження таких вітчизняних науковців, як: О. Амелін, Н. Ахтирська, П. Біленчук, В. Бутузов, В. Голубев, В. Гавловський, С. Демедюк, М. Літвінов, В. Пилипчук, М. Погорецький, В. Шеломенцев, В. Хахановський та інші. Водночас, 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 сучасних тенденцій кіберзлочинності, у тому числі організованих її форм.

**Виклад основного матеріалу.** Тривалий час у чинному законодавстві України було відсутнє нормативно-правове закріплення ключових термінів, зокрема таких, як “кіберзлочин” і “кіберзлочинність”, що спричиняло численні дискусії як серед науковців, так і практиків – співробітників правоохоронних органів.

Законом України “Про основні засади забезпечення кібербезпеки України”, який набув чинності 9 травня 2018 року, визначено, що кіберзлочин (комп'ютерний злочин) – це 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, а кіберзлочинність – сукупність кіберзлочинів [4]. Водночас повного переліку злочинів, передбачених Кримінальним кодексом України, які слід вважати кіберзлочинами, на сьогодні поки що не існує.

Кіберзлочини, на відміну від традиційних, мають низку характерних особливостей, серед яких слід зазначити такі:

- місце вчинення кіберзлочину, на відміну від традиційних, може знаходитись в різних юрисдикціях – правопорушник активізує кібератаку, наприклад, з Інтернет-кафе однієї країни, бот-мережа знаходиться в іншій, а атакована інформаційна система – у третій;
- переважна кількість доказів кіберзлочинів існують в електронній формі (так звані “електронні” або “цифрові” докази). Вони, на відміну від традиційних, можуть швидко знищуватися чи модифікуватися. Для їх отримання, зберігання та аналізу необхідне спеціалізоване обладнання;
- внаслідок специфічної природи кіберпростору постраждалих не завжди обізнаний про вчинення кіберзлочину тощо.

До кіберзлочинів слід віднести не тільки злочини, об'єктом яких є комп'ютерні дані інформаційних систем, але й інші злочини, які вчиняються з використанням кіберпростору. До таких, наприклад, слід віднести торгівлю наркотиками через Інтернет, поширення дитячої порнографії, протиправні дії з платіжними картками тощо.

Кіберзлочинність, як уже зазначалося, завдає значних збитків. Так, масштабна хакерська атака у червні 2017 року, що здійснювалася за допомогою вірусної програми “Petya.A”, порушила роботу багатьох важливих українських державних і приватних підприємств, зокрема: аеропорту Бориспіль, Укртелекому, ЧАЕС, Укрзалізниці, Кабінету Міністрів України тощо. Експерти Міжнародного валютного фонду підрахували, що економічні втрати від атаки вірусу “NotPetya” склали \$ 850 млн. [5].

Сьогодні практично всі фахівці визнають, що ситуація з кіберзлочинністю у світі має сталу тенденцію до погіршення. При цьому посилюється зв'язок між кіберзлочинністю та організованою злочинністю. Інтернет використовують уже не тільки як допоміжний засіб, а й як місце та основний засіб вчинення традиційних злочинів – шахрайства, крадіжок, вимагання.

Однією з причин посилення організованості злочинної діяльності в мережі Інтернет можна вважати те, що така деструктивна діяльність стає більш вигідною, ніж інші способи незаконного збагачення. Експерти вказують на тривожну тенденцію: за останні роки кіберзлочинність стала більш організованою і набула ознак бізнесу, у якому важливими складовими є прибуток та опанування нових ринків.

Завдяки відсутності кордонів протиправна діяльність поширюється на нові регіони в усьому світі. Координація злочинної діяльності здійснюється на будь-яких відстанях з високою швидкістю. Відбувається зрощення національних злочинних угруповань з транснаціональними злочинними організаціями.

Посиленню організованості кіберзлочинності в сучасних умовах сприяють дві взаємопов'язані складові: по-перше, організована злочинність намагається використовувати кіберпростір у своїх цілях, по-друге, складний характер кіберзлочинів змушує осіб, які спеціалізуються на вчиненні злочинів у мережевому інформаційному просторі, координувати свої дії, об'єднуватися і створювати організовані кримінальні співтовариства.

У поле зору оперативних підрозділів дедалі частіше потрапляють організовані злочинні групи зі складною структурою, що мають транскордонні зв'язки. Зростає не тільки організованість кримінальних груп, але і їх законспірованість, збільшується кількість осіб, що займаються протиправною діяльністю в Інтернеті на професійній основі, посилюється спеціалізація таких осіб.

Організовані злочинні угруповання у своїй діяльності часто використовують мережу “Даркнет” (англ. DarkNet) [6], веб-сайти якої не індексуються і на які неможливо потрапити через пошукові системи, такі, як Google чи Yahoo. У “Даркнеті” широко використовуються криптографічні технології мережевої анонімності і он-лайн-розрахунків, які дозволили злочинцям створити чорний ринок, де продають і купують наркотики, крадені і контрафактні товари, дитячу порнографію, зброю тощо.

На даний час ця частина Інтернету ніяк не врегульована законодавчо, діяльність у ній майже неможливо проконтролювати, а тому організовані злочинні угруповання, використовуючи цю мережу, удосконалюють протиправну діяльність. У “Даркнеті” існує велика кількість хакерських спільнот, які спеціалізуються у своїй діяльності за конкретними напрямками, наприклад, неправомірний доступ до комп'ютерних систем, продаж шкідливого програмного забезпечення (далі – ШПЗ), організація кібератак, викрадення та продаж персональних даних тощо.

Такі приховані ринки самі по собі організовують злочинні співтовариства. Вони мають великих і дрібних функціонерів. Основна відмінність від традиційних організацій полягає в тому, що члени віртуальної організації, ймовірно, ніколи не зустрічалися один з одним і не знають один одного в реальності. Вони відомі під “ніком” (вигаданим ім'ям) та аутентифіковані онлайн-історіями і посиланнями на них інших користувачів сайту.

Як приклад функціонування транснаціональної злочинної групи, можна навести протиправну діяльність з торгівлі персональними даними в мережі “Даркнет”, організованої громадянином України. У 2018 році працівники Департаменту кіберполіції Національної поліції України встановили чотирьох українців, які причетні до створення, організації та адміністрування однієї із найвідоміших у мережі “Даркнет” он-лайн-платформи з продажу персональних даних користувачів мережі. До документування цієї злочинної групи були залучені правоохоронці Домініканської Республіки, Індонезії, Іспанії, Франції та України.

Хакери упродовж останніх п'яти років безперешкодно отримували доступ до облікових записів “PayPal”, “Amazon”, “eBay”, “Wells Fargo”, “Suntrust”, “Bank of



America”. Постраждалими від їхніх дій стали як громадяни України, так і мешканці Канади, Великобританії, Іспанії, Франції.

Для отримання такого доступу вони використовували спеціально створене шкідливе програмне забезпечення. Серед інформації, яка поширювалася, були логіни, паролі, персональні дані користувачів, номери їх телефонів, реквізити банківських карток та інші необхідні для авторизації дані. Наприклад, у результаті злому однієї із соціальних мереж, зловмисники отримали дані майже з півмільярда облікових записів.

Отримавши перелік таких записів, хакери використовували спеціалізовані скрипти для визначення облікових записів, які дають доступ до банківських акаунтів та веб-сайтів електронної комерції. Приблизний загальний річний обіг он-лайн-платформи становив майже 22 млн. доларів США.

Працівники кіберполіції провели санкціоновані обшуки на території трьох регіонів України в Одеській та Волинській областях, а також у місті Києві. За їх результатами вилучено комп’ютерну техніку, мобільні телефони та чорнові записи. Вилучену техніку направлено на експертизу.

Кримінальне провадження розпочато за ч. 2 ст. 361 (“Несанкціоноване втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку”) КК України [7].

Для посилення боротьби з кіберзлочинністю Європол у 2013 році створив Європейський центр кіберзлочинності (англ. European Cybercrime Centre, далі – ECC). З моменту свого створення ECC вніс значний внесок у боротьбу з кіберзлочинністю, брав участь у десятках великих операцій і здійснював сотні операцій з оперативної підтримки, що призвело до багатьох арештів злочинців.

Починаючи з 2014 року, ECC щорічно готує та оприлюднює Звіт про оцінку загроз організованої кіберзлочинності (англ. Internet Facilitated Organised Crime Threat Assessment, далі – ІОСТА) [8]. У звіті досліджуються тенденції та нові загрози, які впливають на уряди, бізнес та громадян ЄС. Аналітичні матеріали для ІОСТА готуються на основі досліджень експертів Європолу, правоохоронних органів, партнерів з приватного сектору та наукового середовища.

У звіті приділяється увага сферам злочинності, що належать до компетенції ECC. До них відносяться: кіберзлочини (кібератаки, зловмисне програмне забезпечення, бот-мережі та ін.), сексуальна експлуатація дітей в Інтернеті, шахрайство з платіжними картками (викрадення даних карток – “кардінг”, “скімінг”). До інших напрямів, які аналізуються ІОСТА, належать так звані наскрізні чинники злочинів, які охоплюють багато сфер злочинності, але самі по собі не завжди є кримінально караними діями. Зокрема, це зловживання криптовалютами, відмивання брудних коштів, отриманих злочинним шляхом, компрометація корпоративної електронної пошти тощо.

Метою доповідей ІОСТА є інформування осіб, відповідальних за прийняття рішень на стратегічному, політичному та тактичному рівнях у сфері боротьби з кіберзлочинністю для спрямування оперативної діяльності правоохоронних органів ЄС, а також інформування громадськості про реальні та потенційні загрози у кіберпросторі, можливі сценарії реагування на них, здобутки правоохоронних органів ЄС у сфері боротьби з кіберзлочинністю.

Доповідь ІОСТА готується групою стратегічних аналітиків Європолу, яка у своїй роботі спирається переважно на матеріали держав-членів ЄС, Цільової групи Європейського союзу з кіберзлочинності (далі – EUCTF), аналітичних проектів Європолу “Cyborg”, “Terminal” і “Twins”, а також групи кіберрозвідки (англ. Cyber Intelligence Team) та групи SOCTA у вигляді структурованих досліджень, опитувань та

модерованих семінарів. Також у доповіді використовуються результати досліджень з відкритих джерел та внески від приватного сектору, включаючи консультативні групи ECC, Євроюст, ENISA, CERT-EU, EBF та спільноту CSIRT. Ці внески відіграють ключову роль у підготовці доповіді. Водночас на сьогодні в Україні такого дослідження проведено ще не було.

Аналіз матеріалів ІОСТА за 2016 – 2018 роки дозволяє визначити наступні тенденції організованої кіберзлочинності:

1) Розповсюдження програм-вимагачів (“Ransomware”) становить одну з основних загрозу у кіберпросторі. Вони поширили свій вплив на різноманітні галузі як у державному, так і в приватному секторах. При цьому успіх та попит на програми-вимагачі призвів до різкого зростання (на 750 % за 2 роки) кількості їх сімейств.

Активне розповсюдження таких програм пояснюється тим, що порівняно з іншими шкідливими програмами, які викрадають інформацію, програми-вимагачі легше монетизувати (отримати викуп), а також за допомогою криптовалют (наприклад Bitcoin) здійснити подальше відмивання таких злочинних грошей. Крім того, за допомогою програми-вимагача можна атакувати значно різноманітніший спектр цілей, тобто майже будь-кого, хто зберігає конфіденційні дані.

Незважаючи на те, що об'єктами кібератак є, у переважній більшості, звичайні люди, їхніми цілями стають також малі та середні підприємства, яким часто бракує ресурсів для повного захисту своїх даних та мереж.

Деякі напади були спрямовані на критичні національні інфраструктури (лікарні, правоохоронні органи, державні установи та служби) та створили безпосередню загрозу життю громадян. Серія кібератак “WannaCry” у травні 2017 року стала яскравим прикладом втручання у роботу лікарень у Великобританії, порушення функціонування залізничної мережі в Німеччині, телекомунікаційних компаній в Іспанії та Португалії, нафтохімічних компаній в Китаї та Бразилії.

Поєднання факторів, що стояли за атаками середини 2017 року “WannaCry” та “NotPetya”, призвели до того, що національні правоохоронні органи усвідомили свою неспроможність самотійно протидіяти таким кібератакам та необхідність більшої та посиленої співпраці між правоохоронними органами різних країн, компаніями приватного сектору, науковими колами та іншими відповідними зацікавленими сторонами.

В 2016 році для боротьби з програмами-вимагачами правоохоронними органами ЄС (ECC, поліція Нідерландів) у співпраці з приватним сектором був створений і впроваджений у роботу портал “No More Ransom” [9]. Метою цієї ініціативи є широке інформування громадськості про небезпеки, пов'язані з програмами-вимагачами, і надання допомоги жертвам даного ШПЗ у відновленні своїх даних без сплати викупу зловмисникам. Даний портал діє і сьогодні для підвищення обізнаності та забезпечення безкоштовними засобами дешифрування постраждалих від кібератак.

2) Поширення DDoS-атак.

Продовжуються DDoS-атаки на державні та приватні організації, у т.ч. на критичну інфраструктуру. Зокрема, у 2018 році одна третина держав-членів ЄС повідомила про випадки нападу на критичну інфраструктуру.

Спостерігається зростання інтенсивності та складності DDoS-атак, поширюються пропозиції “DDoS-атака як послуга” (англ. DDoS-as-a-service).

Як правило в організації потужних кібератак задіяна значна кількість виконавців. Так у грудні 2016 року Європол та правоохоронні органи з Австралії, Бельгії, Франції, Угорщини, Литви, Нідерландів, Норвегії, Португалії, Румунії, Іспанії, Швеції, Сполученого Королівства Великобританії та Сполучені Штати Америки здійснили

скоординовані дії, орієнтовані на користувачів сервісу DDoS-атаки, що призвело до 34 арештів та допиту 101 підозрюваних осіб.

Сьогодні, на відміну від попередніх років, вимоги, що висуваються під час таких атак, мають не лише корисливий, а й політичний та ідеологічний характер, що не виключає безпосередню участь у такій діяльності спонсорованих державою організованих злочинних угруповань.

Для протидії таким атакам правоохоронні органи повинні зосередитися на суб'єктах, які розробляють та надають засоби для кібератак, зокрема банківські трояни та інші шкідливі програми, а також на постачальниках засобів для DDoS-атаки, служб бот-мережі тощо.

Небезпечним в експертному середовищі вважається також динамічний розвиток "Інтернету речей" (англ. Internet of Things, IoT, далі – IP). З'явилися DDoS-атаки, що походять від бот-мереж компрометованих пристроїв IP. До 2020 року прогнозується зростання кількості таких кібератак на 25 %. В Україні також прогнозується поширення IP. Для оперативного обговорення проблем щодо розвитку IP в Інтернет-асоціації України створена відкрита група фахівців [10].

Традиційно метою злочинних організацій є кошти банківських установ.

У березні 2018 року в місті Аліканте в Іспанії заарештували лідера злочинного угруповання 34-річного українця К. Дане угруповання розпочало свою діяльність у 2013 році, здійснюючи кібератаки на банки, системи електронних платежів та фінансові установи, використовуючи свої власні розробки, відомі як "Carbanak" і "Cobalt".

За даними слідства, постраждалими від злочинної діяльності злочинних угруповань стали понад 100 банків з 40 країн. Однак основні крадіжки були здійснені ним в банках Росії. За попередніми даними, сума викраденого перевищує 1 мільярд євро, хоча мова може йти і про значно більшу суму (до 10 мільярдів). Пізніше у США арештували ще трьох громадян України – членів злочинного угруповання "Carbanak" або ж "Fin7" [11].

3) Незважаючи на те, численна аудиторія споживачів користується мережею Tor та іншими подібними анонімізуючими мережами для розповсюдження незаконних товарів, розширилася сфера використання мережі "DarkNet" у напрямку реалізації наркотичних та психотропних речовин, зброї, засобів ураження, скомпрометованих платіжних даних, дитячої порнографії, підроблених документів тощо.

У квітні 2017 року Європол та Інтерпол надавали підтримку іспанській національній поліції у проведенні операції "Tantalo" з комплексного розслідування поширення дитячої порнографії через мережу "DarkNet". Спільні слідчі дії проводилися у 5 країнах Європи під керуванням Європолу та в 13 країнах Центральної та Південної Америки за координації Інтерполу. В результаті операції було заарештовано 39 підозрюваних у Європі та Південній Америці.

У червні 2017 року Європол організував проведення кампанії "Скажи НІ" (англ. Say NO) [12], спрямованої на допомогу потенційним жертвам сексуальної експлуатації дітей, надання он-лайн-консультацій з метою отримання навичок із розпізнавання спроб примусу до такої експлуатації та шляхів звернення за допомогою до компетентних національних органів у разі вчинення таких злочинів.

Станом на червень 2017 року в мережі "Tor" було понад 2,2 мільйона безпосередньо підключених користувачів і майже 60 тис. унікальних доменів ".onion". Проблему становить лише кількісне визначення співвідношення незаконної активності в цих мережах до законного їх використання звичайними користувачами для більш безпечного перегляду веб-сторінок. Майже 57 % активних засекречених сайтів пов'язані з певною формою незаконної діяльності [12].

Загалом можна констатувати, що наразі найбільш динамічно збільшується кількість кіберзлочинів, спрямованих на мобільні платформи, в яких протягом останніх років удвічі зросла кількість виявлень зловмисного програмного забезпечення.

Ще однією загрозою у світі є масштабне впровадження у більшості країн криптовалют, які стають повноцінним платіжним засобом та інвестиційним активом. Зацікавленість до використання криптовалют сприяє інвестиційній привабливості платіжних інфраструктур. Проте “Bitcoin” та інші цифрові валюти адаптовані для використання організованими злочинними угрупованнями, оскільки вони досить поширені в міжнародному обігу та забезпечують необхідний рівень анонімності. Маючи спеціальні технічні навички та вміння, міжнародні терористичні угруповання можуть використовувати віртуальні валюти для фінансування терористичних заходів. Загроза відмивання грошей, пов’язаних з віртуальними валютами, демонструє, що кримінальний світ може використовувати віртуальні валюти для доступу до “чистої готівки” і одночасно приховувати сліди транзакцій.

Водночас криптовалюти є також ціллю кіберзлочинців. За повідомленням “Reuters”, з криптобірж у ході кібератак за перші 9 місяців 2018 року вивели 927 мільйонів доларів, що на 250 % більше, ніж за весь 2017 рік. У компанії відзначають, що дослідження базується на офіційних даних, реальні ж цифри можуть бути набагато вищі [13].

Щодо труднощів, пов’язаних з проведенням слідчих дій, які стосуються розслідувань кіберзлочинів, слід зазначити зростаючу ступінь витонченості злочинної діяльності та необхідність для слідчих органів бути обізнаними в сучасних технологіях так само, як кіберзлочинці. Адже кібератаки стають дедалі складнішими, їх дедалі важче виявити, і в той же час ці методи швидко знаходять вихід до широкого загалу користувачів.

Зростання кількості кіберзлочинів обумовлюється удосконаленням технічних і програмних засобів, доступних для зловмисників, і посилюється існуванням нелегального ринку з продажу засобів для здійснення кіберзлочинів.

Зростаюча ступінь витонченості злочинної діяльності викликає ще більші труднощі, пов’язані з виявленням електронних доказів, застосуванням зловмисниками методів заплутування, необхідністю аналізу великих обсягів даних і отриманням даних від постачальників послуг.

Функції зберігання інформації в цифровій формі і використання глобальної мережі дедалі частіше інтегруються в звичайні предмети побуту і особистого вжитку, такі як ручки, камери, годинник з флеш-пам’яттю і ювелірні прикраси з USB-накопичувачами. Крім того, бездротові пристрої зберігання можуть бути заховані в поглибленнях стін, в надстелевому просторі і під підлогою. Той факт, що комп’ютерні дані фізично легко заховати, створює труднощі для розслідування.

Останнім часом рівень кіберзлочинності швидко зростає і в Україні. Експерти зазначають, що Україна – дуже важливий центр хакерства, поряд із Бразилією, Китаєм та меншою мірою – Індією.

Відповідно до статистичних даних, наданих Національною поліцією України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням високих інформаційних технологій за останній рік збільшилося на 36 %.

Вже у 2019 році працівники Поліського управління Департаменту викрили групу осіб у створенні вірусів та їх використанні для незаконного збагачення. Зловмисники створили бот-мережу, яка сканувала та перебирала паролі до комп’ютерів для отримання повного контролю над ними. Отримавши доступ, в тому числі і до он-лайн-

банкінгу, хакери перераховували усі кошти з рахунків власника інфікованого комп'ютера на підконтрольні рахунки. Зловмисники змогли отримати таким способом понад 5 млн. гривень [14]. Кримінальне провадження розпочато за декількома статтями кримінального кодексу України: ст. 361 ("Несанкціоноване втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку") та ст. 185 ("Крадіжка") КК України.

В Україні також продовжується розповсюдження шкідливого програмного забезпечення. Наприклад, у м. Глухів громадянин А. здійснював продаж шкідливого програмного забезпечення для викрадення паролів через різноманітні форуми та через програми Skype і Telegram. Слобожанським управлінням кіберполіції НП України було встановлено також, що даний громадянин організував свій відеоблог на YouTube, на якому розповідається про використання шкідливого програмного забезпечення.

Для отримання коштів від покупців правопорушник використовував заборонені в Україні платіжні системи. Кримінальне провадження розпочато за статтею 361-1 КК України [15].

Правоохоронні органи України виявляють непоодинокі випадки несанкціонованого доступу до державних баз даних.

Так у лютому 2019 року працівники Департаменту внутрішньої безпеки та Головного слідчого управління Національної поліції України, під процесуальним керівництвом Генеральної прокуратури України, викрили колишнього начальника одного з департаментів Національної поліції України в організації схеми незаконного збагачення шляхом продажу службової інформації. Полковник поліції разом зі спілниками тривалий час за грошову винагороду надавав конфіденційні відомості та безпосередній доступ до них колекторським конторам, мережі банківських установ і приватним підприємствам. За легалізовані кошти чиновник придбав 9 квартир у столиці.

Готується оголошення підозри 6 учасникам організованого злочинного угруповання за ч. 3 ст. 28 (скоєння злочину групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією), ч. 2 ст. 361 (несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку) і ч. 2 ст. 361-2 (несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації) Кримінального кодексу України [16].

Також продовжуються розробка та розповсюдження усіляких шахрайських схем, які вчиняються з використанням мережі Інтернет.

Усі схеми діяльності шахраїв схожі між собою. Як приклад, вже у 2019 році кіберполіція припинила діяльність офісу, який позиціонував себе як "бінарний опціон". Зловмисники, під виглядом участі в он-лайн торгах валютними парами ("бінарні опціони") пропонували бажаним отримання додаткового пасивного прибутку. Для цього необхідно було створити свій робочий он-лайн кабінет на сайті "dax100.org" та зробити внесок – 100 євро.

Коли ж клієнт намагався вивести гроші, шахраї під різними приводами відмовляли в цьому та пропонували продовжити торги. Якщо клієнт відмовлявся й надалі вкладати кошти в торги, адміністрація майданчика цілеспрямовано проводила ряд операцій, що призводили до повної втрати клієнтом грошей.

За оперативною інформацією, у 2018 році тисячі громадян як України, так і за кордоном, стали жертвами подібних схем. За приблизними оцінками, в Україні один шахрайський офіс протягом місяця приносив близько мільйона гривень. Найбільші з

них – “HQbroker” та “Trade12”. Протягом року в Україні кіберполіція припинила діяльність 18 злочинних груп. За усіма цими фактами розпочато кримінальні провадження та триває досудове розслідування [17].

Водночас за даними судової статистики, у 2017 році за статтями, передбаченими Розділом XVI КК України (ст. 361 – 361-3), засуджено лише 42 особи: з яких 5 осіб позбавлено волі на строк до 3 років та 2 особи – на строк від 3 до 5 років, тобто часто покарання за вчинення кіберзлочинів обмежується тільки невеликим штрафом – тому, що ці злочини кваліфікуються як середньої тяжкості.

А дані судової статистики за 2018 рік вказують на те, що з 70 засуджених осіб позбавлено волі лише 3, серед яких так само як і в попередньому році **тільки 2 особи позбавлено волі на строк до 5 років**.

При цьому варто зазначити, що цей вид злочинів (учинених повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду) в Україні максимально карається позбавленням волі на строк від трьох до шести років.

В той же час за повідомленням ЗМІ українські хакери засуджуються в різних державах за протиправну діяльність в кіберпросторі на строки від 30 – 40 років і більше позбавлення волі. Наприклад, членів організованого злочинного угруповання “Western Express”, яка спеціалізувалася на викраденні платіжних карток, і до якої входив громадянин України Ш., у 2013 році було засуджено Верховним судом штату Нью-Йорк до 40 років позбавлення волі [18].

Сьогодні, на думку фахівців, жоден комплексний кримінологічний аналіз не здатний дати повного уявлення про глобальні масштаби кіберзлочинності, у тому числі організованих її форм, що суттєво відрізняється від традиційної.

Розглянувши комплекс проблем у сфері забезпечення кібербезпеки та констатуючи її кризовий стан, що загрожує національній безпеці, Рада національної безпеки і оборони України своїм Рішенням від 29 грудня 2016 року “Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації”, введеним в дію Указом Президента України від 13 лютого 2017 року №32/2017, зобов’язала Кабінет Міністрів України у тримісячний строк внести в установленому порядку на розгляд Верховної Ради України законопроекти щодо імплементації положень Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, передбачивши, низку організаційних заходів, серед яких на сьогодні залишається невиконаним запровадження дієвого механізму використання в кримінальному процесі доказів в електронній формі, зібраних у процесі здійснення оперативно-розшукової діяльності. У зв’язку з цим особливого значення набуває повна імплементація Конвенції про кіберзлочинність [19].

У зв’язку з подальшим поширенням використання у злочинній діяльності інформаційних технологій правоохоронним органам також слід розробляти нові підходи у боротьбі з новими видами злочинної діяльності та створювати відповідні організаційні структури. Наприклад, ФБР створило відділ боротьби з високотехнологічною організованою злочинністю (англ. Hi-Tech Organized Crime Unit, далі – НТОСУ), основним завданням якого є аналіз та дослідження проблем і загроз від діяльності організованих злочинних угруповань, які використовують передові технології у незаконної діяльності.

Це дасть змогу не тільки розробити стратегічні рекомендації, але й посилити координацію правоохоронних органів, зосередившись на глобальних загрозах, що виникають від організованих злочинних угруповань. НТОСУ співпрацює з “Cyber Division” ФБР для підготовки слідчих до розслідування діяльності організованих злочинних угруповань “під прикриттям” в Інтернеті та у співпраці з Міжнародним

центром розвідки та операцій з організованою злочинністю (англ. The International Organized Crime Intelligence and Operations Center – IOC-2) розробляє он-лайн-платформу для дослідження протиправної діяльності у “Даркнеті” тощо [20].

### **Висновки.**

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

Для посилення боротьби з кіберзлочинністю, у тому числі її організованим формам пропонується:

- враховуючи тяжкі наслідки, які можуть бути завдані вчиненням кіберзлочинів, ініціювати питання щодо посилення санкцій за вчинення злочинів, передбачених статтями 361, 361-1, 361-2, 362, 363, 363-1 КК України, доповнивши ці статті відповідними частинами, що дасть змогу перевести їх у розряд тяжких злочинів, посилить кримінальну відповідальність за їх вчинення, а також розширить перелік негласних слідчих (розшукових) заходів, що можуть бути проведені для їх припинення або документування;
- законодавчо унормувати поняття “криптовалюта” для можливості притягнення до відповідальності осіб за вчинення злочинних дій з їх використанням;
- посилити державно-приватне партнерство у протидії кіберзлочинності, у тому числі при підготовці нормативно-правових документів у цій сфері;
- внести зміни до Глави 4 Докази і доказування Кримінального процесуального кодексу України в частині порядку отримання, зберігання, оцінки та передачі електронних доказів під час судового та досудового розслідувань;
- підготувати аналітичний звіт ІОСТА в Україні, який мав би велике значення для виконання Угоди між Європолом та Україною щодо стратегічного співробітництва та сприяв ефективному впровадженню положень Стратегії кібербезпеки України.

### **Використана література**

1. Internet World Stats. URL: <https://www.internetworldstats.com/emarketing.htm> (дата звернення: 07.12.2018).
2. Украинская аудитория Facebook выросла на 3 млн человек за 2018 год, общее количество пользователей соцсети в нашей стране составляет 13 млн. URL: [https://itc.ua/news/ukrainskaya-auditoriya-facebook-vyirosla-na-3-mln-chelovek-za-2018-god-obshhee-kolichestvo-face-book-polzovateley-teper-sostavlyaet-13-mln-infografika/#disqus\\_thread](https://itc.ua/news/ukrainskaya-auditoriya-facebook-vyirosla-na-3-mln-chelovek-za-2018-god-obshhee-kolichestvo-face-book-polzovateley-teper-sostavlyaet-13-mln-infografika/#disqus_thread) (дата звернення: 19.02.2019).
3. Киберпреступники наживаются на самых бедных. URL: <https://www.unodc.org/unodc/ru/frontpage/2018/May/much-work-to-do-and-no-time-to-waste-in-cybercrime-fight--says-un-chief.html> (дата звернення: 19.02.2019).
4. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. URL: <http://zakon2.rada.gov.ua/laws/show/2163-19> (дата звернення: 07.09.2018).
5. Збитки від глобальних кібератак у світі сягнули \$ 53 мільярдів – МВФ. URL: <https://www.ukrinform.ua/rubric-world/2322816-zbitki-vid-globalnih-kiberatak-u-sviti-sagnuli-53-mil-ardiv-mvf.html> (дата звернення: 07.09.2018).
6. Гуцалюк М.В. Протидія використанню учасниками злочинних угруповань мережі “Даркнет”. *Інформація і право*. № 3(26)/2018. С. 102-108.
7. Кіберполіція припинила діяльність одного з найвідоміших майданчиків у DarkNet із продажу персональних даних. URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-prypnyla-diyalnist-odnogo-z-najvidomishykh-majdanchykyv-u-darknet-iz-prodazhu-personalnykh-danykh-4672> (дата звернення: 27.12.2018).

8. Internet Organised Crime Threat Assessment (IOCTA). URL: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment> (дата звернення: 27.12.2018).
9. No More Ransom. URL: <https://www.nomoreransom.org/ru/index.html> (дата звернення: 19.02.2019).
10. В Україні взяли за популяризацію Інтернету вещей. URL: <http://internetua.com/v-ukraine-vzyalis-za-populyarizaciua-interneta-veshei> (дата звернення: 19.02.2019).
11. У США арештували українських хакерів. URL: <https://www.pravda.com.ua/news/2018/08/1/7188031> (дата звернення: 27.12.2018).
12. Internet Organised Crime Threat Assessment (IOCTA) 2017. URL: <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>
13. Хакери вкрали з криптобірж майже 1 мільярд доларів з початку року. URL: <https://www.epravda.com.ua/news/2018/10/11/641522> (дата звернення: 27.12.2018).
11. Рынок киберкриминала: спрос втрое превышает предложение. URL: <http://channel4it.com/publications/Rynok-kiberkriminala-spros-vtroe-prevyshaet-predlozhenie-31263.html#> (дата звернення: 27.12.2018).
12. Here's how easy it is to buy anything – legal or illegal – on the 'dark web'. URL: <https://www.businessinsider.com/find-anything-on-dark-web-tor-internet-2016-11>.
- Hacking communities in the Deep Web. URL: <https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref> (дата звернення: 07.09.2018).
13. Cryptocurrency Attacks Are Rising. URL: <https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw> (дата звернення: 07.09.2018).
14. Кіберполіція викрила групу хакерів, які ошукали українців більш як на 5 мільйонів гривень. URL: <https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-grupu-xakeriv-yaki-oshukaly-ukr-ayincziv-bilsh-yak-na--miljoniv-gryven-968> (дата звернення: 19.02.2019).
15. Українському видеоблогеру грозит два года тюрьмы за продажу вирусів. URL: <http://internetua.com/ukrainskomu-videoblogeru-grozit-dva-goda-tuarmy-za-prodaju-virusov> (дата звернення: 19.02.2019).
16. Екс-начальник Нацполіції купив дев'ять квартир на відмиті від продажів баз даних МВС гроші. URL: <https://ukranews.com/ua/news/615126-eks-nachalnyk-natspolitsiyi-kupyv-dev-yat-kvartyr-na-vidmyti-vid-prodazhiv-baz-danyh-mvs-groshi> (дата звернення: 19.02.2019).
17. Кіберполіція фіксує збільшення випадків шахрайств, вчинених під виглядом інвестування на фінансових ринках. URL: <https://www.npu.gov.ua/news/kiberzlochyni/kiberpolicziya-fiksuje-zbilshennya-vipadkiv-shahrajstv-vchinenix-pid-viglyadom-investuvannya-na-finansovix-rinkax> (дата звернення: 19.02.2019).
18. США: приговоры по делу хакеров из России и Украины. URL: [https://www.bbc.com/russian/international/2013/08/130812\\_usa\\_hackers\\_carders\\_sentences](https://www.bbc.com/russian/international/2013/08/130812_usa_hackers_carders_sentences) (дата звернення: 19.02.2019).
19. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.05 р. № 2824-IV. URL: [https://zakon.rada.gov.ua/laws/show/994\\_575](https://zakon.rada.gov.ua/laws/show/994_575) (дата звернення: 27.12.2018).
20. Organized Crime Has Gone High Tech. URL: <http://www.policechiefmagazine.org/organized-crime-has-gone-high-tech> (дата звернення: 27.12.2018).

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


УДК 342.951

ТКАЧУК Н.А., кандидат юридичних наук,
старший науковий співробітник НДІП НАПрН України

СТАН ТА ПРОБЛЕМНІ ПИТАННЯ РЕАЛІЗАЦІЇ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

Анотація. У статті досліджено стан і проблемні питання реалізації Стратегії кібербезпеки України та запропоновано шляхи удосконалення стратегічного планування у сфері кібербезпеки держави.

Ключові слова: Стратегія кібербезпеки України, план реалізації Стратегії кібербезпеки України, кібербезпека, стратегічне планування, нормативно-правове регулювання.

Summary. The article examines the state and problematic issues of implementing the Cybersecurity Strategy of Ukraine, and suggests ways to improve the strategic planning in the field of cybersecurity of the state.

Keywords: the Cybersecurity Strategy of Ukraine, Ukraine's Cybersecurity Strategy Implementation Plan, cyber security, strategic planning, legal regulation.

Аннотация. В статье исследуется состояние и проблемные вопросы реализации Стратегии кибербезопасности Украины, а также предложены пути усовершенствования стратегического планирования в сфере кибербезопасности государства.

Ключевые слова: Стратегия кибербезопасности Украины, план реализации Стратегии кибербезопасности Украины, кибербезопасность, стратегическое планирование, нормативно-правовое регулирование.

Постановка проблеми. Протягом останніх років в Україні триває активна розбудова національної системи кібербезпеки, що обумовлено перетворенням кіберпростору на невід'ємну складову суспільного життя у поєднанні з актуалізацією кіберзагроз життєво важливим інтересам держави, правам та свободам громадян в умовах гібридної агресії з боку Російської Федерації.

Фундаментом дієвої системи кібербезпеки, безумовно, є ефективна нормативно-правова база, основою якої в Україні стала ухвалена у березні 2016 року "Стратегія кібербезпеки України" (далі – Стратегія) [1].

Стратегія забезпечила підґрунтя для розроблення подальших нормативно-правових актів з питань кібербезпеки та визначила основні засади та напрями державної політики у цій сфері. Кожного року Розпорядженням Кабінету Міністрів України затверджується річний план заходів з її реалізації, який включає конкретні завдання для органів державної влади, спрямовані на виконання положень Стратегії, вирішення існуючих проблемних питань та розбудову кібербезпекового потенціалу України.

Разом з тим, сьогодні в державі відсутній механізм оцінки ефективності реалізації Стратегії, а більшість заходів, передбачених планами її реалізації на 2016 – 2018 роки, залишаються невиконаними. Ситуація, що склалася, негативно впливає на стан та ускладнює формування дієвої державної політики у цій царині, зводить нанівець ефективність документів стратегічного планування кібербезпекової сфери.

Результати аналізу наукових публікацій. Проблематика правового регулювання сфери кібербезпеки України висвітлювалася у наукових працях О. Довганя, Д. Дубова, Р. Лукиячука, А. Марущака, М. Ожевана, В. Петрова, В. Пилипчука, В. Шеломенцева та

ін. вітчизняних дослідників. Проблеми стратегічного планування у сфері державного управління вивчалися такими вітчизняними вченими як А. Гнатенко, О. Берданова, М. Латинін, О. Лебединська, М. Лесечко, І. Лех, Т. Тарасюк, Ю. Шаров та ін. Водночас, слід констатувати, що питання реалізації Стратегії кібербезпеки України залишилося поза увагою комплексних наукових досліджень. На практиці це призводить до недооцінення ролі документів стратегічного планування, як однієї із важливих складових організаційно-правової основи функціонування національної системи кібербезпеки та формування державної кібербезпекової політики.

Метою статті є визначення стану та проблемних питань реалізації Стратегії кібербезпеки України на сучасному етапі.

Виклад основного матеріалу. Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики у сфері кібербезпеки. Вказаний документ є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [2].

Цей документ є базисом стратегічного планування держави у сфері кібербезпеки, що за своєю суттю є адаптивним процесом, за допомогою якого повинні здійснюватись регулярні розроблення й корекція системи планів, перегляд змісту заходів щодо їх виконання на основі безперервного контролю й оцінки змін, які відбуваються ззовні та всередині системи [3, с. 55].

Контроль за виконанням стратегій, досягненням цільових орієнтирів, а також їх коригування сучасна теорія державного управління визначає як невід'ємний елемент стратегічного управління. Як зазначає Г. Тарасюк, роль контролю як функції управління полягає в тому, що він є засобом здійснення зворотного зв'язку в системі управління. Головний його сенс полягає у створенні гарантій виконання планових рішень [4, с. 290].

Разом із тим, в Україні дієва система стратегічного контролю, яка б забезпечувала об'єктивну оцінку та здійснення корегуючого впливу щодо стану реалізації Стратегії кібербезпеки, а також гарантій виконання її положень, на сьогодні відсутня.

Наразі реалізація положень Стратегії відбувається в рамках виконання щорічних планів, які формуються Держспецзв'язку України та затверджуються відповідними Розпорядженнями Кабінету Міністрів України. Водночас, аналіз стану виконання на загальнодержавному рівні планів реалізації Стратегії кібербезпеки України на 2016 – 2018 роки [5 – 7], проведений автором, засвідчив, що вказані документи носять переважно декларативний характер. Так, більшість заходів, передбачених ними, наразі, не виконано або виконано частково та/або із простроченням встановлених термінів. Кінцевий результат наявний лише щодо деяких із пунктів. Наприклад, прийнято Закон України “Про основні засади забезпечення кібербезпеки України”, створено Ситуаційний центр забезпечення кібербезпеки СБ України, удосконалено вимоги до захисту інформації в ІТС банківської сфери (шляхом прийняття відповідного відомчого нормативно-правового акту НБУ¹).

Багато інших важливих питань на сьогодні не вирішено: не створено перелік інформаційно-телекомунікаційних систем критичної інфраструктури, не імplementовано Конвенцію ЄС про кіберзлочинність, не побудовано захищений дата-центр для органів державної влади, не вжито ефективних заходів щодо стимулювання розроблення

¹ Постанова Правління НБУ “Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України” від 28.09.17 р. № 95.

вітчизняного програмного забезпечення, не впроваджено регламенти та директиви щодо стандартів ЄС із захисту об'єктів критичної інфраструктури, відсутня система аудиту інформаційної безпеки таких об'єктів, не сформовано основні індикатори стану кібербезпеки та показники ефективності виконання Стратегії кібербезпеки України, не створено єдину систему виявлення кіберзагроз та платформу обміну інформацією (даними) між суб'єктами кібербезпеки тощо.

Хоча всі пункти планів, якими були передбачені ці завдання, містили конкретні кінцеві дати виконання та відповідальних за їх виконання державних суб'єктів. Наприклад, відповідальним органом за виконання 15-ти пунктів із наявних 18-ти, передбачених Планом реалізації Стратегії кібербезпеки України на 2018 рік (затвердженим розпорядженням КМУ від 11.07.18 р. № 481-р), є Державна служба спеціального зв'язку та захисту інформації України.

Крім того, своєчасне та ефективне виконання заходів з реалізації Стратегії значно ускладнює той факт, що плани її реалізації формуються Держспецзв'язку України, і відповідно, затверджуються Урядом із порушенням встановленого рішенням РНБО України терміну (до початку планового року) [1].

Так, план реалізації Стратегії на 2017 рік було затверджено КМУ у березні 2017 року (із простроченням терміну на 3 місяці), а на 2018 рік – у липні 2018 року (із простроченням терміну на 7 місяців). Станом на березень 2019 року (під час написання даної статті) план реалізації Стратегії на 2019 рік також відсутній. Ситуація, що склалася, апriorі унеможливорює своєчасне виконання окремих планових позицій суб'єктами кібербезпеки.

Наприклад, відповідно до Розпорядження КМУ “Про затвердження плану заходів на 2018 рік з реалізації Стратегії кібербезпеки” від 11.07.18 р. № 481-р [7], звітувати про хід виконання Плану необхідно було до 10 липня 2018, незважаючи на те, що цей план було затверджено на день пізніше строку звітування. Цей приклад ілюструє абсурдність ситуації, яка склалася у сфері стратегічного планування та контролю за виконанням заходів з реалізації Стратегії кібербезпеки України.

Безумовно, для того, щоб існуючі законодавчі та підзаконні нормативно-правові акти мали не лише декларативний характер, а дійсно були фундаментом подальшої реалізації конкретних заходів у сфері забезпечення кібербезпеки, необхідно запровадити дієвий механізм контролю щодо їх своєчасного та належного виконання всіма без виключення суб'єктами забезпечення кібербезпеки України. А у разі не виконання – повинен працювати механізм дієвого реагування та вжиття відповідних заходів правового впливу та притягнення до відповідальності.

Відповідно до чинних нормативно-правових актів², суб'єктами, на які покладені завдання із здійснення контролю із цього питання, є Секретар РНБО України (у частині забезпечення контролю за виконанням указу Президента України, яким затверджена Стратегія кібербезпеки) [8] та Секретаріат Кабінету Міністрів України (у частині забезпечення контролю та моніторингу стану виконання розпоряджень КМУ, якими затверджуються щорічні плани реалізації Стратегії) [9]. Крім того, питання стану реалізації Стратегії кібербезпеки України щорічно розглядається на засіданні Національного координаційного центру кібербезпеки, який повинен забезпечувати координацію діяльності суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки

² Положення про порядок організації та здійснення контролю за виконанням указів, розпоряджень і доручень Президента України, затвердженого Указом Президента України від 19.02.02 р. № 155, та Регламенту Кабінету Міністрів України, затвердженого Постановою Кабінету Міністрів України від 18.07.07 р. № 950.

України, підвищувати ефективність системи державного управління у формування та реалізації державної політики у сфері кібербезпеки [10].

Водночас, основні завдання стратегічного контролю із надання об'єктивної оцінки та вжиття заходів впливу щодо неналежної реалізації Стратегії кібербезпеки відповідальними суб'єктами, на сьогодні, не здійснюються, а невиконані завдання просто переносяться на наступний рік (про що свідчить аналіз планів реалізації Стратегії на 2016 – 2018 роки).

Крім того, не створені умови, які б забезпечили можливість ефективного контролю за станом реалізації Стратегії кібербезпеки з боку громадянського суспільства. Закон України “Про національну безпеку” [2] визначає дотримання засад демократичного цивільного контролю (одним із елементів якого є громадський контроль) за функціонуванням сектору безпеки і оборони одним із основних принципів формування державної політики у всіх сферах національної безпеки. Предметом такого контролю визначено стан реалізації стратегій, доктрин, концепцій, державних програм та планів у сферах національної безпеки і оборони, тобто у т.ч. Стратегії кібербезпеки України. Наявність дієвого громадського контролю є невід'ємною умовою демократії та ознакою правової держави.

Водночас, здійснення такого контролю у сфері кібербезпеки ускладнює відсутність відповідної публічної інформації з боку компетентних державних органів, в першу чергу Державної служби спеціального зв'язку і захисту інформації України, як органу, на який покладено завдання із узагальнення інформації про хід виконання планових заходів із реалізації Стратегії кібербезпеки України, а також Національного координаційного центру кібербезпеки. Сприяти вирішенню цього питання могло б оприлюднення на офіційних веб-ресурсах вказаних органів узагальнених матеріалів щодо стану та конкретних результатів діяльності суб'єктів національної системи кібербезпеки із виконання планів реалізації Стратегії з урахуванням вимог Закону України “Про державну таємницю”.

Відповідно до основоположних засад державного управління невід'ємною умовою ефективності стратегічного планування є обов'язковий стратегічний моніторинг, саме на підставі якого має відбуватися корегування основних цілей та завдань стратегічних документів [11]. Планування щорічних заходів з реалізації Стратегії кібербезпеки України має ґрунтуватися на оцінці поточного стану реалізації Стратегії, конкретних результатів виконання планових заходів за попередні періоди, а також аналізі стану кіберзахисту та кібербезпеки держави.

Законом України “Про національну безпеку” запроваджено проведення комплексного огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, підготовка якого покладена на Держспецзв'язку України. У контексті кібербезпеки цей огляд і повинен, у тому числі, відігравати функцію стратегічного моніторингу та бути основою подальшого розроблення документів стратегічного планування кібербезпекової сфери.

Водночас, незважаючи на вимоги закону, підготовка вказаного огляду, на сьогодні, зазначеним відомством не проводилася, що негативно впливає на якість стратегічного планування у сфері кібербезпеки та кіберзахисту.

Також відсутня методика формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України, створення якої відповідно до розпоряджень Кабінету Міністрів України мало бути вже завершене Державною службою спеціального зв'язку та захисту інформації України.

Зокрема, планом реалізації Стратегії кібербезпеки України на 2017 рік (пунктом 15) було передбачено протягом 2017 року здійснити *“формування переліку основних показників ефективності виконання Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик”* [6]. Планом реалізації Стратегії на 2018 рік (пунктом 13) знову передбачалось здійснити *“розроблення методики формування та визначення основних показників ефективності реалізації Стратегії кібербезпеки України з урахуванням досвіду європейських і світових практик”* вже протягом 2018 року [7]. Але ні у 2017, ні у 2018 роках ці завдання виконані не були (відповідальний за їх виконання орган – Держспецзв’язку). Отже, на сьогодні, будь-яка офіційна методика та показники ефективності виконання Стратегії кібербезпеки України відсутні, що фактично дозволяє уникати проведення відповідальним органом огляду стану її виконання, результати якого, вочевидь, продемонструють неефективність та формальний підхід до реалізації документів стратегічного планування в державі.

Сьогодні в державі поступово починається процес розроблення проекту нової Стратегії кібербезпеки України на 2021 – 2025 роки. Однак, без здійснення належної оцінки та вирішення проблемних питань щодо стану реалізації існуючої – така робота лише засвідчить формальний підхід до стратегічного планування у сфері кібербезпеки та пріоритетність не результату, а власне, процесу заради процесу. В умовах гібридної агресії та необхідності протистояння кіберзагрозам Україна собі це дозволити не може.

Висновки.

1. На сьогодні, стан реалізації Стратегії кібербезпеки України є незадовільним, що негативно впливає на всю сферу кібербезпеки та кіберзахисту України та є свідченням формального підходу з боку відповідальних державних органів до стратегічного планування, формування та реалізації державної політики, а також здійснення стратегічного контролю у цій сфері.

2. З метою підвищення ефективності стратегічного планування та сприяння належній реалізації Стратегії кібербезпеки пропонується:

- терміново розробити критерії та започаткувати впровадження механізму оцінки ефективності реалізації Стратегії кібербезпеки України на державному рівні;
- провести передбачений Законом України “Про національну безпеку України” огляд стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, який обов’язково повинен враховуватись у ході подальшої розробки документів стратегічного планування кібербезпекової сфери та здійснення оцінки їх реалізації;
- запровадити дієвий контроль з боку Кабінету Міністрів та РНБО України та щодо своєчасного та якісного виконання компетентними державними органами завдань, спрямованих на реалізацію Стратегії кібербезпеки України, із здійсненням (або ініціюванням) заходів дисциплінарного впливу щодо відповідальних посадових осіб, які не забезпечили їх належне виконання;
- систематично розмішувати інформацію на офіційних веб-ресурсах Держспецзв’язку України та Національного координаційного центру кібербезпеки при РНБО України щодо стану виконання відповідальними державними органами поточних планів реалізації Стратегії кібербезпеки України та отриманих кінцевих результатів (з урахуванням вимог Закону України “Про державну таємницю”);
- забезпечити своєчасне (до початку звітного періоду) формування Держспецзв’язку України та, відповідно, затвердження Урядом щорічних планів реалізації Стратегії кібербезпеки України.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про стратегію кібербезпеки України”: Указ Президента України. URL: <http://zakon.rada.gov.ua/laws/show/96/2016>
2. Про національну безпеку України: Закон України від 21.06.18 р. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
3. Гнатенко А.І. Стратегічне планування у сфері державного управління: концептуальні підходи. *Державне управління та місцеве самоврядування*: зб. наук. пр. Дніпропетровськ: Вид-во ДРІ НАДУ. 2013. № 3(18). С. 51-60.
4. Тарасюк Г.М. Контроль в системі управління плановою діяльністю підприємства. *Міжнародний збірник наукових праць*. 2010. № 1(16). С. 284-299.
5. Про затвердження Плану заходів на 2016 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 24.06.16 р. № 140-р. URL: <https://zakon.rada.gov.ua/laws/show/440-2016-%D1%80>
6. Про затвердження Плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.17 р. № 155-р. URL: <http://zakon2.rada.gov.ua/laws/show/155-2017-%D1%80>
7. Про затвердження Плану заходів на 2018 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 11.07.18 р. № 481-р. URL: <https://zakon.rada.gov.ua/laws/show/481-2018-%D1%80>
8. Про порядок організації та здійснення контролю за виконанням указів, розпоряджень і доручень Президента України: Указ Президента України від 19.02.02 р. № 155. URL: <https://zakon.rada.gov.ua/laws/show/155/2002>
9. Про затвердження Регламенту Кабінету Міністрів України: Постанова Кабінету Міністрів України від 18.07.07 р. № 950. URL: <https://zakon.rada.gov.ua/laws/show/950-2007-%D0%BF>
10. Президент затвердив Положення про Національний координаційний центр кібербезпеки. URL: <https://www.president.gov.ua/news/prezident-zatverdiv-polozhennya-pro-nacionalnij-koordinacijn-37329>
11. Назаров В.П. Стратегічне планування як важливий чинник підвищення ефективності державного управління. *Влада*. 2013. № 12. С. 4-11.

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

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

УДК 347.91(477): 347.633

**ТУБОЛЬЦЕВА Я.С.**, аспірант кафедри цивільного процесу,

Національний юридичний університет імені Ярослава Мудрого

**ВИКЛЮЧНІ ОСОБЛИВОСТІ РОЗВИТКУ ІНСТИТУТУ УСИНОВЛЕННЯ  
У ВІТЧИЗНЯНОМУ ЦИВІЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ПРАВІ**

**Анотація.** У статті досліджено процес зародження інституту усиновлення в Україні з найдавніших часів на підставі аналізу чинної в різні історичні періоди нормативно-правової бази та наукової літератури. Виявлено існування різних форм усиновлення на кожному окремому етапі розвитку державності та суспільного життя, що конкретно залежали від правил оформлення та компетенції органу, що наділений таким правом законодавцем того чи іншого часу. Зроблена спроба навести хронологічну послідовність становлення даного інституту у цивільному процесуальному праві України та виокремити характерні особливості, що зумовлені специфікою впливу законодавства зарубіжних держав.

**Ключові слова:** становлення законодавства, історичний розвиток, нормативно-правове регулювання, усиновлення, цивільне судочинство, судовий порядок.

**Summary.** The article examines the process of the commencement of the adoption institution in Ukraine since ancient based on the analysis of the legislation and scientific literature current in different historical periods. The existence of various forms of adoption at each separate stage of development of statehood and social life, which specifically depended on the rules of registration and competence of the body, which is endowed with such a right by the legislator at that time, has been identified. An attempt is made to bring the chronological sequence of the formation of this institute in the civil procedural law of Ukraine and to distinguish the characteristic features that are caused by the specifics of the influence of the legislation of foreign countries.

**Keywords:** formation of legislation, historical development, legal regulation, adoption, civil proceedings, judicial procedure.

**Аннотация.** В статье изучается процесс зарождения института усыновления в Украине с древнейших времен на основе анализа действующей в разные исторические периоды нормативно-правовой базы и научной литературы. Установлено, что на каждом отдельном этапе развития государства и общественной жизни существовали различные формы усыновления, которые конкретно зависели от правил оформления и компетенции органа, который был наделен таким правом законодателем того времени. Сделана попытка привести хронологическую последовательность становления данного института в гражданском процессуальном праве Украины и выделить характерные особенности, обусловленные спецификой влияния законодательства зарубежных государств.

**Ключевые слова:** становление законодательства, историческое развитие, нормативно-правовое регулирование, усыновление, гражданское судопроизводство, судебный порядок.

**Постановка проблеми.** Усиновлення, як форма влаштування дітей-сиріт та дітей, позбавлених батьківського піклування, є одним із найстаріших, класичних, але досить складним інститутом права, оскільки окремі його елементи регулюються різними

галузями права. Визначення особливостей врегулювання процесуальних питань усиновлення неможливе без врахування історичного досвіду розвитку його основних засад як інституту права. Слід врахувати, що з часу введення в дію оновленого Цивільного процесуального кодексу України (далі – ЦПКУ), за правилами цього нормативно-правового акту судами загальної юрисдикції розглядалось 8933 справи та матеріалів зазначеної категорії. Тому, з урахуванням застосування історичного підходу наукового дослідження, зміст якого вдало розкритий в роботі О.Г. Данильяна та О.П. Дзюбаня, вважаємо за необхідне проаналізувати особливості розвитку інституту усиновлення у вітчизняному цивільному процесуальному законодавстві [1, с. 296].

**Результати аналізу наукових публікацій.** Питання інституту усиновлення розглядалися у правовій літературі з позиції історико-правового дослідження, становлення у сімейному праві, а також етапи розвитку цивільного процесуального права, таким вченими як Г.І. Вершиніна (H.I. Vershynina), І.В. Ковальчук (I.V. Kovalchuk), В.В. Комаров (V.V. Komarov), Н.П. Косенко (N.P. Kosenko), М.В. Логвінова (M.V. Lohvinova), О.В. Розгон (O.V. Rozghon), З.В. Ромовська (Z.V. Romovska), та багато інших. Разом з тим, відсутнє спеціальне комплексне дослідження історії становлення і розвитку інституту усиновлення в цивільному процесуальному праві України.

**Метою статті** є визначення передумов формування та процесу становлення інституту усиновлення у цивільному процесуальному праві України на різних історичних етапах.

**Виклад основного матеріалу.** Усиновлення має довгу історію становлення як правового явища. Розуміння його змісту було закладено ще в давнину, а згодом розвивалося та зустрічалося в законодавчих приписах стародавніх держав. Хоча усиновлення тісно пов'язано із нормами римського цивільного права, його процедура не була ретельним чином закріплена в нормативних актах того часу. Так, усиновлення отримало суто юридичну форму і розглядалося як встановлення батьківської влади над чужими дітьми з виникненням відносин, подібних спорідненості.

В Стародавній Русі діяла важлива пам'ятка українського права “Руська Правда”, що не виділяла норм щодо регулювання усиновлення. В основі такої процедури з часів Київській Русі були норми звичаєвого права та обряди: “переродження” або обряд фіктивного народження (імітувати пологи міг і чоловік); одруження з вдовою брата; фактичний прийом усиновленого до будинку; особливий договірний акт між усиновителем і особою, що усиновлюється. Згодом, після хрещення Русі (988 р.) церква поступово почала брати на себе те, раніше регулювалось звичаєвим правом. Усиновлення здійснювалося церквою та освячувалося особливим церковним обрядом, який називався “слинотворення” [2, с. 32-33].

Таким чином, процес усиновлення того часу мав так звану звичаєву або примітивну форму. Така процедура регулювалася нормами звичаєвого права й гарантувалася засадами тогочасного суспільства, здебільшого всі процесуальні дії здійснювались в усній формі або певного обряду, порядок вчинення учасниками процесу дій при розгляді та вирішенні справи не мав чіткого визначення, а витікав із логіки самого обряду, та, як результат, не відображався у спеціальних документах.

Довгий час норми й процедура усиновлення не піддавались змінам. Як відомо, внаслідок поділу Польщі, російсько-турецьких війн, ліквідації козацтва українські землі на початок ХІХ ст., опинилися під владою Російської та Австрійської імперій.

Усиновлення на західноукраїнських землях було досить поширеним суспільним явищем, яке визначалося довгий час звичаєвим правом. Робота над кодифікацією цивільного та інших галузей права в останній чверті ХVІІІ ст. призвела до прийняття



Галицької книги законів 1797 г., а згодом – Цивільний кодекс для всієї Австрії був затверджений імператорським патентом і з 1 січня 1812 р введений в дію під назвою “Загальне цивільне уложення для спадкових земель Австрійської монархії” [3, с. 228].

Питанням усиновлення було присвячено статті 179 – 186 глави III “Про взаємні права батьків і дітей” вищевказаного нормативного акту. Під час усиновлення між сторонами обов’язково мав укладатися договір, що мав бути затверджений у судовому засіданні. Ця вимога встановлювалася для того аби попередити незаконне усиновлення, а також переконатися, що сторони витримали всі вимоги закону. Відповідно до §185 Загального цивільного уложення Австрійської імперії 1811 р. договір про усиновлення можливо було розірвати лише внаслідок взаємної домовленості сторін, причому виключно в такій формі, в якій його було укладено. Та, незважаючи на введення в дію Австрійського цивільного кодексу, на українських землях продовжували діяти норми звичаєвого права. Таким чином, в період з 1829 до 1920 рр. було розглянуто 26 справ про встановлення опіки над дітьми-сиротами і жодної справи про усиновлення [4, с. 70-74 ]. Цікаво, що на території вже сучасної західної держави Австрійське загальне цивільне уложення 1811 р. зі змінами та доповненнями є чинним і досі.

На українських землях у складі Російської імперії законодавство про усиновлення стало розвиватися так, як і на західноукраїнських землях на початку XIX ст., хоча у нормах права XVIII ст. вже зустрічався інститут усиновлення. В Указі Петра I 1714 р. “Про єдиноспадкування” та Інструкції про магістрати 1724 р. про усиновлення згадувалося лише стосовно передачі спадкоємцям майна спадкодавця [5, с. 17]. Згідно з “Правами, за якими судиться малоросійський народ” 1743 р., усиновлення – це правовий акт, за яким батьки брали чужих дітей як своїх природних й допускали їх до спадщини (Гл. XIII, арт. 14, п. 1). На жаль, цей документ не врегульовував безпосередньо процедуру усиновлення, але, як стверджує І.В. Ковальчук, безумовно мав значний вплив на становлення правового інституту усиновлення на українських землях [6, с. 14].

Таким чином, не зважаючи на те, що усиновлення знайшло вже нормативного закріплення у законодавстві, не була розроблена детальна процедура розгляду справи. Тобто, відсутність певної послідовності вчинення судом та учасниками процесу процесуальних дій та, крім того, фіксування цих дій у процесуальних документах, не могло не позначатись на реалізації самого усиновлення.

Сві розвиток законодавство, присвячене усиновленню, отримало на початку XIX століття. Олександр I видав Указ 11 жовтня 1803, що дозволяв дворянам, у яких були відсутні свої діти, всиновлювати найближчих закононароджених родичів “через передачу їм за життя прізвища та герба” та зрівнював спадкові права усиновлених дітей з правами рідних. Протягом всього XIX століття усиновлення зберігало принцип становості й кожен раз оформлялося індивідуальним актом імператора. У наступні роки було видано ряд нормативних актів, що регламентували умови та порядок усиновлення для різних станів (з 1817 р. надається право бездітним громадянам всиновлювати кількох близьких родичів з привласненням їм свого прізвища; 12 січня 1828 р. – приписка купців і міщан до власного звання підкинутих дітей, тих, хто не пам’ятає споріднення, та осіб, що перебувають на вихованні, законодавчо визнається формою усиновлення) [7, с. 245].

Введений в дію 1 січня 1835 р. Том X Зводу Законів Російської імперії у частині першій Звод законів цивільних продовжував охороняти принцип становості. Відділення п’яте “О дітях усиновлених” (ст. 145 – 151) Глави першої Розділу другого Книги першої встановлювало правові норми, що регулювали інститут усиновлення тієї доби [8]. Правова регламентація процесуальних питань знайшла своє відображення в Статуті

цивільного судочинства 1864 року (далі – СЦС 1864 р.). Так, судова реформа 1864 р. Олександра II внесла великі зміни в судоустрій і судочинство тогочасної імперії.

Спочатку Статут складався з чотирьох книг, а з квітня 1866 р. впроваджувались правила неспірного або охоронного порядку судочинства з доповненням Статуту Книгою IV, що мала назву “Судочинство охоронне”. Так, правила про посвідчення судом договірної угоди між особами про усиновлення були введені в судові статuti лише Законом від 12 березня 1891 р. “Про дітей усиновлених і узаконених” і впроваджені зі змінами до закону від 3 червня того ж року, а згодом законом від 3 червня 1902 р. “Про поліпшення становища незаконнонароджених дітей” [9, с. 488-506]. Відділ книги охоронного провадження, що містив регламентацію процедури розгляду справ про усиновлення (Розділ VII ст. 1460-8 і 1460-12), було складено членом Остасгожского окружного суду Е.І. Гельвіхом. Необхідно відзначити, що за СЦС 1864 р. розрізнялося усиновлення та узаконення дітей, причому узаконити можливо було лише своїх дітей, а усиновити – своїх та чужих.

Подальший огляд законодавства вказує на те, що усиновлення регулювалося в основному нормами матеріального права. Правила, встановлені СЦС 1864 р., передбачалися тільки для дворян та осіб привілейованих станів. Для інших осіб був спрощений порядок усиновлення в залежності від станової приналежності: селяни та міські жителі – з дозволу казенної палати шляхом приписки дитини до сімейства усиновителя, особи козацьких чинів та нижчі військові чини – по розпорядженню начальства цих чинів [8].

Для дворян процедура усиновлення складалася з декількох етапів. Спочатку здійснювалася у нотаріуса складання акту про усиновлення, надалі подавалась звернення до суду з дозволом про усиновлення, а після судової процедури- підтвердження цього акту судовою палатою.

Сам процесуальний порядок усиновлення також мав свої особливості. Прохання про усиновлення подавалося в окружний суд за місцем постійного проживання або усиновителів, або усиновленої дитини (ст. 1460-1 СЦС 1864 р.), а де не було окружних судів – усиновлення здійснювалося судовими місцями. Розглядалися справи про усиновлення суддею окружного суду одноособово. У проханні (заяві) про усиновлення було достатнім вказати на те, що усиновлена дитина дійсно не перебуває вже в усиновленні у іншої особи. Подання доказів на підтвердження цього факту законом не було встановлено. З проханням про усиновлення дитини могли звернутися тільки особи, які бажали стати батьками по відношенню до усиновлюваного.

Окружному суду, що розглядав справу про усиновлення, мали бути представлені дані, що офіційно засвідчують наявність згоди всіх учасників усиновлення (ст. 149 Зводу законів цивільних). Згоду на усиновлення могло бути виражено підпискою в судовому засіданні, в проханні на ім’я суду або в іншому документі від осіб, які виявили згоду (ст. 1460-9 СЦС 1864 р.). Воля усиновителя остаточно виражалася в проханні про усиновлення і не потребувала підтвердження перед судом.

Суду також повинні бути надані відомості щодо дотримання інших, встановлених ст.ст. 145-151 Зводу законів цивільних, умов: вік (усиновитель має бути не молодшим за 30 років й бути старшим за усиновленого на 18 років), сімейний стан (не дозволялося усиновлювати особам, які за сном своїм приречені на “безбраччє”), релігія (заборонялося усиновлення християн нехристиянами), згода іншого з подружжя при усиновлення одним із них.

При розгляді клопотання про усиновлення окружним судом опікунські установа мала представити “посвідчення”, яке підтверджує, що усиновлення не звернеться на шкоду усиновлюваної дитини [10, с. 287].

Результатом розгляду справи було винесення судом ухвали про задоволення клопотання або про відмову в задоволенні, після збору всіх вищевказаних матеріалів й вислухавши висновок прокурора. Усиновлення вважалося таким, що відбулося з дня набрання ухвалою суду законної сили. Дану ухвалу можна було оскаржити до Судової палати в порядку охоронного провадження. Відповідно до СЦС 1864 р. зі скаргою на ухвалу окружного суду у справах про усиновлення мав право звернутися і прокурор. Особам, права яких порушувались неправильним усиновленням, надавалося право заперечувати під час провадження у справі або розпочати власний спір за правилами позовного провадження протягом 2 років від дня набрання ухвалою суду законної сили, але за умови, що усиновитель був ще живий [9, с. 510].

Аналіз вищевикладеного дає підстави стверджувати про те, що саме в той період відбулося зародження цивільної процесуальної форми справ про усиновлення як врегульованого нормами цивільного законодавства порядку вчинення судом, особами, які беруть участь у справі процесуальних дій у процесі розгляду та вирішення даної категорії справ охоронного провадження, а також оформлення таких дій у процесуальних документах. Як вірно стверджувала Н.О. Чечіна, будь-яке судочинство, повне чи спрощене, здійснюється в межах процесуальної форми, за відповідними процесуальними правилами, на основі загальних принципів, закріплених процесуальним законодавством [11, с. 185]. Також, слід звернути увагу, що деякі елементи механізму правового регулювання досліджуваного періоду простежуються в чинному матеріальному та процесуальному законодавстві.

Наступним етапом було введення в дію Кодексу законів про акти громадянського стану, шлюбне, сімейне і опікунське право від 22 жовтня 1918 р., яким на майбутнє інститут усиновлення скасовувався, й такі правила діяли до 1 березня 1926 року, коли російська влада видала Декрет ВЦВК і РНК РРСФР “Про зміну Кодексу законів про акти громадянського стану, шлюбне, сімейне і опікунське право” й було введено главу “Про усиновлення” (ст. 182-183.9).

В той період на території України 30 червня 1919 року Рада Народних Комісарів (РНК) Української РСР прийняла Сімейний кодекс УРСР, який так і не набув чинності через воєнні дії в державі, але, на відміну від сімейного законодавства РРСФР, містив дві статті про усиновлення, а процесуальна сторона питання залишилася поза увагою. Так, в ті часи на Українській РСР усиновлення не заборонялось і вже з початку 1920 року суди почали приймати рішення про усиновлення [12, с. 59].

Важливим моментом в історії розвитку цивільного процесуального права є схвалення ВУЦВК 30 липня 1924 р. і набуття чинності 1 жовтня 1924 р. Цивільного процесуального кодексу Української СРР, як першого основного систематизованого джерела радянського процесу в Україні у ті роки. Пізніше у 1929 р., у зв’язку із змінами в адміністративно-територіальному устрої, було прийнято оновлений Цивільний процесуальний кодекс, однак зазначений документ порядок здійснення усиновлення не визначав.

В Українській РСР уперше повноцінного законодавчого регулювання досліджуваній інститут набуває, також як і в РРСФР, 31 травня 1926 року з прийняттям на 3-й сесії ВУЦВК 9-го скликання Кодексу законів про сім’ю, опіку, подружжя та про акти громадянського стану Української РСР.

Таким чином, з 1926 року відповідно до Положень Розділу I гл. 5 “Усиновлення (удочеріння)” вищевказаного документа вирішення питання про усиновлення було делеговано опікунським установам, і така практика тривала аж до 1996 року.

Усиновлення за заявою усиновителя проводилось органами опіки і піклування за місцем проживання усиновителя, шляхом перевірки обставин його проживання та усиновленого задля переконання, що цей акт не буде здійснено з метою експлуатації неповнолітніх, а також усиновитель зможе представити умови для нормального фізичного та духовного розвитку усиновленого. Так само усиновитель повинен був пред’явити медичну довідку про стан свого здоров’я та здоров’я членів своєї сім’ї, з якими він разом проживає та з якими буде проживати усиновлений (ст. 41 Кодексу законів про сім’ю, опіку, подружжя та про акти громадянського стану Української РСР 1926 р.).

Усиновлення обов’язково реєструвалося в загальному порядку реєстрації актів громадянського стану. Реєстрація проходила в містах та в районних центрах та здійснювалась міськими та районними відділами (бюро) записів актів громадянського стану, а в сільській місцевості і робочих селищах – сільським і селищними радами, й була безкоштовною [13, с. 56].

В окремих випадках, скасування усиновлення могло бути здійснене за рішенням суду на підставі заяви державного органу, громадської організації або приватної особи, якщо цього вимагали інтереси дитини. Така заява подавалась до органу опіки, який потім вирішував питання щодо подальшого руху заяви.

У судовому порядку могло також розглядатися питання встановлення факту реєстрації усиновлення відповідно до редакції вищевказаного кодексу від 1954 року. Так, дана процедура здійснювалась за умови неможливості отримання заінтересованою особою документів на підтвердження зазначеного факту чи за умови неможливості відновлення втрачених або знищених документів. Справи розглядалися народними судами за заявою заінтересованих осіб за місцем їх проживання. Законодавством не допускалося встановлення факту усиновлення в судовому порядку, якщо усиновлений або усиновитель помре до того часу, як усиновлення було оформлено належним чином [13, с. 69].

Наступним кроком було затвердження Верховною Радою СРСР 8.12.1961 р. (введені в дію з 1.05.1962 р.) Основ цивільного судочинства Союзу РСР і союзних республік та прийняття на його основі 18 липні 1963 р. Верховною Радою УРСР нового Цивільного процесуального кодексу УРСР, що був введений в дію 1 січня 1964 р. Також, Кодексом про шлюб та сім’ю Української РСР від 30 липня 1969, який був введений Указом Президії Верховної Ради Української РСР від 17 жовтня 1969 року “Про порядок і введення в дію Кодексу про шлюб та сім’ю Української РСР”, як й вищевказаними кодифікованими актами, був збережений адміністративний порядок усиновлення.

Так, усиновлення допускалося лише щодо неповнолітніх дітей за рішенням виконавчого комітету районної чи міської ради народних депутатів (згодом районної, міської адміністрації). Цей нормативно-правовий акт вперше закріплював заходи забезпечення таємниці усиновлення.

Кодекс передбачав можливість скасування усиновлення, а також визнання його недійсним, тільки в судовому порядку на підставі заяви державного органу, громадської організації чи приватної особи, якщо цього вимагали інтереси дитини. При розгляді таких справ необхідним було подання письмового висновку органів опіки і піклування,

а також участь в судовому засіданні представника цього органу й прокурора. У зв'язку з цим зверталася увага на правові наслідки таких дій.

Отже, у радянський період разом із адміністративним порядком розгляду справи про усиновлення, існувала диференційована процедура скасування усиновлення: адміністративна, якщо усиновлення здійснювалося за відсутності згоди батьків дитини, та судова, якщо цього вимагали інтереси дитини. Як слушно зазначає Г.І. Вершиніна, поступові зміни інституту усиновлення та скасування усиновлення, що в різні періоди регулювалися нормами матеріального права, до середини 1990-х років послідовно привели законодавця до думки про те, що усиновлення є комплексною категорією, у зв'язку з чим має регулюватися процесуальним та матеріальним законодавством [14, с. 12].

Згодом Президія Верховної Ради Української РСР видає Указ “Про внесення змін і доповнень до Кодексу про шлюб та сім'ю Української РСР” від 1 вересня 1980, після чого ст.160 кодексу встановлювала, що реєстрацію усиновлення на підставі рішення виконавчого комітету проводять відділи запису актів громадянського стану виконавчих комітетів районних, міських, районних у містах Рад народних депутатів.

Наступними актами були інструктивно-методичні рекомендації з питань усиновлення (удочеріння) неповнолітніх для органів народної освіти та охорони здоров'я, що регламентував перелік документів, необхідних для оформлення усиновлення, порядок підготовки матеріалів, реєстрації та ін. [15].

Переломним моментом, що призвів до суттєвих змін у нормативно-правовому регулюванні інституту усиновлення, стало виявлення правоохоронними органами масових фактів незаконного усиновлення дітей України з боку іноземних громадян та проведення розслідування цих кримінальних справ.

Так, усиновлення іноземними громадянами, супроводжувалося численними випадками складання фіктивного документа про смерть новонародженого з метою його продажу за кордон, підміни дітей у пологових будинках, винесення рішення про усиновлення у день звернення, що підтвердились висновком постійної Комісії Верховної Ради України з питань прав людини, національних меншин і міжнаціональних відносин.

Вказані випадки змусили розпочати підготовку змін і доповнень до Кодексу про шлюб та сім'ю 1969 р. Отже, Постановою Верховної Ради України від 26 липня 1994 р. було схвалено у першому читанні проект Закону України “Про внесення змін і доповнень до Кодексу про шлюб та сім'ю”. З тих же причин з цього моменту було накладено тимчасовий мораторій на усиновлення дітей, які є громадянами України, іноземними громадянами.

Законодавцем було прийнято рішення запобігти різного роду порушень – віднести розгляд та вирішення справ про усиновлення до судової юрисдикції. Закон України “Про внесення доповнень до Цивільного процесуального кодексу України у зв'язку з прийняттям Закону України “Про внесення змін і доповнень до Кодексу про шлюб та сім'ю України” (зміни щодо порядку усиновлення дітей)” введено в дію з дня його опублікування – 24 липня 1996 року.

Судовий розгляд, як слушно зазначає В.В. Комаров, максимально забезпечує здійснення процедури усиновлення з дотриманням передбаченого законом порядку шляхом встановлення обставин, з якими закон пов'язує настання відповідних правових наслідків, і тому є гарантією ухвалення законного й обґрунтованого рішення та ефективного захисту прав та інтересів дитини та інших заінтересованих у розгляді справи осіб [16, с. 135]. На сучасному етапі розвитку суспільства такий розгляд є історично виправданим, оскільки не можна не погодитись, що сам інститут усиновлення є досить пластичним, тобто змінювався під впливом певних подій та життєвих реалій в державі.

Найважливішим нормативно-правовим актом в системі регулювання інституту усиновлення в Україні, після Конституції України 1996 року та Сімейного кодексу України від 10 січня 2002 року (набув чинність 1 січня 2004 року), став Цивільний процесуальний кодекс України від 18 березня 2004 р.

На сьогоднішній день, ЦПК України в редакції від 3 жовтня 2017 року детально регулює порядок судочинства в цивільних справах й містить главу “Розгляд судом справ про усиновлення”. Правове регулювання досудового етапу здійснюється на підставі постанови Кабінету Міністрів України “Про затвердження порядку провадження діяльності з усиновлення та здійснення нагляду за дотриманням прав усиновлених дітей” від 8 жовтня 2008 року № 905 та Сімейним кодексом України.

На сучасному етапі розвитку державності Україна стоїть на шляху входження до Європейського Союзу, що передбачає імплементацію європейських стандартів і підходів до забезпечення прав дітей, основні напрями яких визначено Стратегією Ради Європи з прав дитини (2016 – 2021 рр.). Так, Концепція Державної соціальної програми “Національний план дій щодо реалізації Конвенції ООН про права дитини” на період до 2021 року, схвалена розпорядженням Кабінету Міністрів України від 5 квітня 2017 р., налаштована на забезпечення продовження послідовної імплементації положень Конвенції ООН про права дитини та розбудови ефективної системи захисту прав та інтересів дитини.

Як вірно зазначає О.В. Розгон, особливе значення для питання усиновлення має Європейська Конвенція про усиновлення дітей, яку було ратифіковано 15 лютого 2011 року. Ратифікація вказаної Конвенції була також передбачена інтеграцією в Європейський Союз та необхідністю узгодження українського законодавства з європейськими приписами [17, с.139]. Відповідно до ст.4 вказаного міжнародного документа усиновлення вважається дійсним лише за умови, якщо воно вчинене судовим або адміністративним органом (“компетентним органом”).

### **Висновки.**

Підсумовуючи вищевикладене, необхідно звернути увагу, що розбудовуючи власну державу, український народ протягом багатьох століть знаходився під владою інших держав, що позначилось на формуванні вітчизняної нормативно-правової бази, в тому числі щодо усиновлення. Аналіз історичних документів, що діяли на території України в різні часи, дає можливість говорити про несамотійний рецептивний характер законодавства.

Сучасний період також визначає залежність українських поглядів від європейських принципів побудови сім’ї, що позначається на гармонізаційних процесах у сфері регулювання інституту усиновлення.

Таким чином, огляд історичного процесу розвитку процесуального інституту усиновлення на території України вимагає осмислення проблем періодизації з метою позитивного вдосконалення в майбутньому.

### **Використана література**

1. Данильян О.Г., Дзьобань О.П. Організація та методологія наукових досліджень: навч. посіб. Харків: Право, 2017. 448 с.
2. Ковальчук І. В. Передумови виникнення інституту усиновлення на території України. *Вісник Академії адвокатури України*. 2008. № 13. С. 29-34.
3. Стефанчук Р.А. Гражданский кодекс Галиции 1797 г. как одна из первых мировых кодификаций гражданского законодательства. *Часопис цивілістики*. 2016. Вип. 20. С. 227-230.

4. Ковальчук І.В. Становлення інституту усиновлення на території Галичини, Північної Буковини та Закарпаття за часів Австрійської імперії. *Вісник Академії адвокатури України*. 2009. № 1 (14). С. 69-75
5. Косенко Н.П. Становлення та розвиток інституту усиновлення в сімейному законодавстві. *Юридична наука*. 2013. № 12. С. 15-21.
6. Ковальчук І.В. Усиновлення, як соціально-правове явище на території України до середини XVIII ст. *Вісник Академії адвокатури України*. 2013. №1. С. 10-15.
7. Іванова М.М. Становлення і розвиток законодавства України про усиновлення. *LEX PORTUS*. 2018. № 3 (11) С. 241-255.
8. Законодательство России. Свод законов Российской Империи. Изд. в 16-и т. URL: <http://pravo.gov.ru/proxy/ips/?empire&nochache> (дата звернення: 19.08.2018).
9. Энгельман И.Е. Курс русского гражданского судопроизводства. Юрьев, 1912. 632 с.
10. Буянова Е.В. Особенности процессуального порядка усыновления по Уставу гражданского судопроизводства 1864 года. *Актуальные проблемы российского права*. 2007. № 2. С. 284-290.
11. Гражданский процесс: учебник / под ред. В.А. Мусина, Н.А. Чечиной, Д.М. Чечота. Москва, 2000. 313 с.
12. Ковальчук І.В. Особливості правового регулювання усиновлення на українських землях у період становлення радянської державності (1917 – 1926 роки). *Науковий вісник Ужгородського національного університету. Серія: Право*. 2012. № 19. С. 58-61.
13. Кодекс законов о семье, опеке, браке и актах гражданского состояния Украинской ССР: принят 3-й сессией Всеукр. Центр. Исполнительного Ком-та 9 созыва 31 мая 1926 г. Официальный текст с изменениями на 10 окт. 1954 г. и с приложением постатейно-систематизированных материалов. Москва: Гос. изд-во юрид. лит-ры, 1954. С. 102
14. Вершинина Г.И. Процессуальные особенности судопроизводства по делам об усыновлении: автореф. дис. ...канд. юрид. наук. Саратов, 2007. 22 с.
15. Про введення в дію інструктивно-методичних рекомендацій з питань усиновлення (удочеріння) неповнолітніх та застосування їх у практичній діяльності органів народної освіти та охорони здоров'я: Наказ МОЗ СРСР та Держкомосвіти СРСР від 31.01.91 р. № 55/40. URL: <https://zakon.rada.gov.ua/laws/show/v0055400-91> (дата звернення: 18.05.2018)
16. Комаров В.В., Світлична Г.О., Удальцова І.В. Окреме провадження: монографія. Харків, 2011. 312 с.
17. Розгон О.В. Значення імплементації норм міжнародного права щодо усиновлення в національне законодавство. *Альманах міжнародного права*. 2016. № 13. С. 135-142.

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


УДК 340:342.7

ГОЛОВКО О.М., кандидат юридичних наук, старший науковий співробітник
НДІ інформатики і права НАПрН України,
старший викладач кафедри публічного права
НТУУ “КПІ ім. Ігоря Сікорського”

ПРАВО НА ІНФОРМАЦІЮ ЩОДО АЛЬТЕРНАТИВНИХ МЕТОДІВ ВИРІШЕННЯ СПОРІВ

Анотація. У статті досліджуються теоретико-правові засади формування права на інформацію про альтернативні методи вирішення спорів. Запропоновано трактувати дане право як невід’ємну складову права на доступ до правосуддя. Розглянуто проблематику забезпечення конфіденційності при застосуванні альтернативних методів вирішення спорів.

Ключові слова: право на інформацію, права людини, доступ до правосуддя, альтернативні методи вирішення спорів.

Аннотация. В статье исследуются теоретико-правовые основы формирования права на информацию об альтернативных методах разрешения споров. Предложено трактовать данное право как неотъемлемую составляющую права на доступ к правосудию. Рассмотрена проблематика обеспечения конфиденциальности при применении альтернативных методов разрешения споров.

Ключевые слова: право на информацию, права человека, доступ к правосудию, альтернативные методы разрешения споров.

Summary. The article examines the theoretical and legal basis of the formation of right to information about alternative dispute resolution. It is proposed to treat this right as an integral part of the right of access to justice. The issue of ensuring confidentiality in the application of alternative methods of dispute resolution is considered.

Keywords: right to information, human rights, access to justice, alternative dispute resolution methods.

Постановка проблеми. В науковій доктрині неодноразово наголошувалось на тому, що судова система через велику кількість проваджень потребує розвантаження, особливо в частині тих справ, які можуть бути вирішені альтернативними методами розв’язання правових спорів (Alternative dispute resolution, далі – ADR). Ця проблема постає безпосередньо при реалізації особою права на доступ до правосуддя, реалізація якого суттєво ускладнюється через так зване “затягування” процесу.

В даній роботі планується визначити права на інформацію про альтернативні методи вирішення спорів та кореспондуючих їм обов’язків, а також розгляд змісту принципу конфіденційності та проблематику його дотримання в межах застосування практик ADR.

Результати аналізу наукових публікацій. Теоретичною основою в даній сфері є нормативно-правові акти в галузі інформаційного права, міжнародні акти щодо практик відновного правосуддя, а також думки відомих вчених з питань, дотичних предмету статті. У науковому дослідженні використовуються доробки таких науковців як Жаровська І.М., Землянська В.В., Притика Ю.Д., Сакара Н.Ю., Спектор О.М., Ткачук О.С. та інші.

Метою статті є виокремлення права на інформацію про альтернативні методи вирішення спорів, аналіз міжнародної та національної нормативно-правової та науково-методичної бази з даної тематики.

Для досягнення вказаної мети ставилося завдання з'ясувати:

- співвідношення права на інформацію з правом на доступ до правосуддя;
- встановити чи передбачаються на практиці обов'язки щодо забезпечення права на інформацію про альтернативні методи вирішення спорів;
- проблематику дотримання принципу конфіденційності в межах застосування практик ADR.

Виклад основного матеріалу. З аналізу змісту ст. 6 Конвенції про захист прав людини та основоположних свобод [1] можна визначити складові елементи права на судовий захист, яке, на нашу думку, є складовою права на доступ до правосуддя. Воно передбачає:

- 1) право на розгляд справи;
- 2) справедливість судового розгляду;
- 3) публічність розгляду справи та проголошення рішення;
- 4) розумний строк розгляду справи;
- 5) розгляд справи судом, встановленим законом;
- 6) незалежність і безсторонність суду;
- 7) право на розгляд справи. Ознака “розумний строк розгляду справи”, як вже зазначалося раніше, не може бути забезпечена національними судами повною мірою.

Повертаючись до поняття доступу до правосуддя, варто підкреслити, що воно має включати й позасудові методи вирішення спорів, що стає можливим, зокрема, завдяки застосуванню медіації у спрах різних категорій справ. Так Жаровська І.М. зазначає, що доступ до правосуддя охоплює досить широкий спектр заходів та засобів, які забезпечують можливість особі або іншому суб'єкту безперешкодно звернутись до органів правосуддя та отримати захист свого права [2, с. 11]. Проте варто погодитися з думкою, що погляд на правосуддя виключно як на вирішення судом справи по суті в сучасних умовах вже не може бути визнаний таким, що відповідає ролі суду в демократичній державі [1].

Як зауважує Сакара Н.Ю., досліджуючи історичний розвиток цієї проблеми в межах руху “Доступ до правосуддя”, вади й недоступність правосуддя пов'язували:

- а) з перешкодами матеріального характеру, які не давали можливості бідним прошаркам населення звернутися за захистом своїх прав до суду (значні судові витрати, неможливість звернення по допомогу до адвоката та ін.);
- б) з відсутністю спеціальних процедур, які давали б можливість ефективно захищати права й інтереси не окремої особи, а відповідної групи, колективу;
- в) зі складністю, дорожнечою судочинства й дуже повільним розглядом справ у судах, необхідністю введення спеціальних альтернативних процедур для вирішення певних категорій справ [3, с. 16].

Деякі вчені розглядають дотримання досудового порядку врегулювання спору як передумову права на пред'явлення позову [4, с. 207].

Як зазначає Європейський суд з прав людини, право на доступ до правосуддя не є абсолютним та може бути піддано обмеженням [5], особливо коли мова йде про умови прийнятності скарги, оскільки це питання потребує регулювання з боку держави, що користується певною свободою розсуду в цьому плані. Разом із тим обмеження не повинні зменшувати доступ особи таким чином та тією мірою, щоб знецінювалася сама сутність цього права. Обмеження не будуть сумісними з п. 1 ст. 6 Конвенції про захист прав людини і основоположних свобод, якщо вони не переслідують “законної мети” та якщо відсутня “розумна співрозмірність між засобами, що використовуються, та метою, яка переслідується” [6].

З наведеного, на нашу думку, впливає, що запровадження обов'язкового досудового порядку врегулювання спору є допустимим. Однак недотримання його не повинно позбавляти особу права на доступ до правосуддя. Тим більше, щодо першої ознаки, у зарубіжних країнах наявна практика "примусового" зобов'язання сторін до використання таких процедур навіть після відкриття провадження у справі [7].

При цьому досудовий порядок, на думку Притики Ю.В., виявляється у застосуванні альтернативних способів вирішення спору як дотримання обов'язкової умови для звернення до державних юрисдикційних органів, наприклад, обов'язкове застосування процедури медіації перед зверненням до суду [8, с. 751]. Спектор О.М. зазначає, що у разі, якщо застосування способу ADR передбачено в обов'язковому порядку законом, тут вже не йдеться про альтернативність. Хоча вона й визнає, що у країнах, де використання ADR значно поширене, ніж в Україні, законодавець все частіше передбачає обов'язкове застосування процедур з примирення перед зверненням до державного суду [9, с. 63].

Виходячи з вищезазначеного, особі має бути забезпечена можливість застосування практик ADR у випадках, коли це не суперечить законодавству. Однак, не застосування нею такої можливості не повинно унеможливлювати її право на звернення до суду за відновленням порушеного права.

Розглядаючи медіацію як один із видів ADR, варто зазначити, що вона може розглядатися як окрема ланка правосуддя, так й інтегруватися в судову систему. В будь-якому разі це дає можливість зменшити судове навантаження на суддів та скоротити час на розгляд справ. При цьому, як правило, скорочуються особисті витрати громадян та вирішується правовий конфлікт шляхом укладення медіаційної угоди між сторонами, а отже підвищується рівень забезпечення права на доступ до правосуддя. Виходячи з вимог законодавства такий договір за результатами зустрічі сторін конфлікту носить цивільно-правовий характер (глави 52 та 53 Цивільного кодексу України).

Указом Президента України "Про Концепцію вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів" від 10 травня 2006 року, було підкреслено необхідність запровадження позитивного досвіду демократичних держав щодо реституційного правосуддя, яке полягає не у покаранні особи, а у примиренні обвинуваченого і потерпілого за участю посередника (медіатора) і/або у відшкодуванні потерпілому завданої матеріальної та моральної шкоди [10]. Цим документом фактично вперше анонсовано потребу в застосуванні нового формату правосуддя, що може бути реалізовано поза класичною судовою процедурою.

Розглядаючи поняття реституційного правосуддя (Restorative Justice) варто зазначити, що цю дефініцію застосовують щодо кримінальних справ або справ, що стосуються деліктів загалом. Тож, реституційне або відновне правосуддя є процесом вирішення правового конфлікту шляхом фокусування уваги на відновленні заподіяної потерпілим шкоди, породження у правопорушниках почуття відповідальності за їхні дії та також залучення громади до розв'язання цього конфлікту [11, с. 8].

Відновне правосуддя в певній частині межує з альтернативними методами вирішення спорів, а точніше – з деякими його видами, зокрема, з медіацією. Альтернативні форми вирішення спорів, включаючи посередництво чи примирення та судові ADR (наприклад, арбітраж), продовжують поширюватися і дедалі частіше інституціоналізуються, що призводить до їхнього визначення як "відповідного" або "пропорційного" судовому вирішенню суперечки.

Система відновного правосуддя "передбачає, що договір, який враховує суб'єктивне сприйняття справедливості сторонами конфлікту, краще приймається

сторонами і з більшою ймовірністю буде сприяти примиренню, ніж нав'язаний (судом або третейським суддею) договір" [12].

Вважається, що діалог і відновлення справедливості взаємно підсилюють один одного, якщо вони відбуваються синхронно і якщо спроби відновного правосуддя передують або супроводжують застосування формального правосуддя. Неофіційна медіація і діалог є важливими стратегіями, які сприяють відновленню справедливості шляхом гуманізації відносин між сторонами конфлікту.

Право на інформацію про альтернативні методи вирішення спорів. Варто зазначити, що наявність окремого напряму правосуддя, яке не відповідає традиційним уявленням викликає питання про правила взаємодії між ними, в тому числі, в частині формування певних прав та обов'язків сторін, що ускладнюється відсутністю законодавчої бази з цих питань, зокрема, йдеться про відсутність закону про медіацію.

В будь-якому разі зрозуміло одне – нетрадиційність ADR не анулює право особи на доступ до правосуддя, а отже з цього випливає ряд питань:

1) Чи можна розглядати в межах права на доступ до правосуддя право на інформацію про альтернативні методи вирішення спорів як таке, що кореспондує до обов'язку уповноважених осіб повідомити сторонам про можливість альтернативних методів вирішення спорів? Під уповноваженими особами мається на увазі, в першу чергу, представники слідчих органів, адвокатури, прокуратури та суду.

2) Чи є потреба зобов'язати уповноважених осіб повідомляти про ADR в частині реалізації особою права на доступ до правосуддя? Реалізація цього обов'язку має здійснюватись на етапі ознайомлення судом сторін з їх правами та обов'язками, що передбачає фіксування факту ознайомлення сторін з можливістю вирішити правовий спір позасудовими методами.

Інформаційним законодавством нашої держави вже передбачено загальне право на інформацію, яке деталізується залежно від правовідносин, в яких бере участь особа. Так, відповідно до ч. 1 ст. 5 Закону України "Про інформацію", кожен має право на інформацію, що передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

Зазначимо також, що на адвокатів в Україні певною мірою вже покладено обов'язок повідомляти клієнта про можливість застосування ADR, що доречно розглядати в межах реалізації права особи на інформацію. Так, відповідно до ч. 2 ст. 28 Правил адвокатської етики: "адвокат має повідомити клієнта про доступність альтернативних способів розв'язання спорів". Отже, дане положення має трактуватись як таке, що передбачає обов'язок адвоката повідомити клієнта про можливість застосування альтернативних способів розв'язання спорів, в тому числі медіації.

Відповідно до ст. 21 Закону України "Про адвокатуру та адвокатську діяльність" зазначається, що адвокату забороняється:

- 1) використовувати свої права всупереч прав, свобод та законних інтересів клієнта;
- 2) без згоди клієнта розголошувати відомості, що становлять адвокатську таємницю, використовувати їх у своїх інтересах або інтересах третіх осіб;
- 3) займати у справі позицію всупереч волі клієнта, крім випадків, якщо адвокат впевнений у самообмові клієнта;
- 4) відмовлятися від надання правової допомоги, крім випадків, установлених законом.

Посилаючись на п. 3 ст. 21 зазначеного Закону варто визначити, чи буде трактуватися порада адвоката своєму клієнту скористатися однією з позасудових способів

вирішення правового конфлікту такою, яка суперечить правам, свободам та законним інтересам клієнта. Так, президент Спілки адвокатів України, голова ВКДКА Олександр Дроздов, аналізуючи проект закону України “Про медіацію” (реєстраційний номер № 3665), зазначив, що той позбавляє адвоката без належних на те підстав права реалізовувати свої професійні здібності у інших сферах суспільних відносин, наприклад виступати у якості медіатора, тобто обмежує права адвоката [13]. В ч. 3 ст. 7 цього проекту дійсно йдеться про те, що медіатором не може виступати адвокат, представник та/або законний представник сторони медіації. Особа не може виступати адвокатом або представником сторони медіації у справі (провадженні), в якій вона надавала або надає послуги медіаторові.

Зазначимо, що відповідно до Рекомендації Комітету Міністрів Ради Європи державам-членам, які зацікавлені в організації медіації у кримінальних справах № R (99) 19, прийнятої Комітетом Міністрів Ради Європи 15 вересня 1999 року (щодо крим. справ): “Мають бути дотримані певні застереження; сторони повинні мати право на правову допомогу та, у випадку необхідності, на тлумачення, роз’яснення”. Таким чином, ч. 3 ст. 7 проект Закону України “Про медіацію” лише виконує зміст даної Рекомендації щодо права сторони медіації на правову допомогу, а отже неможливості одночасного здійснення ролі медіатора поряд з роллю адвоката, представника та/або законного представника сторони медіації в межах одного й того самого процесу.

Звертаючись до американського досвіду поширення інформації про ADR в діяльності адвокатів варто спиратися на Типові правила професійної поведінки (Model Rules of Professional Conduct). Ряд положень, визначених даними Правилами в редакціях різних років дає можливість зробити висновок про наявність обов’язку адвоката повідомити свого клієнта про альтернативні методи вирішення його спору.

Серед таких положень можна виділити такі:

1) Пункт 1.2 Типових правил передбачає, що адвокат повинен дотримуватися рішення клієнта щодо мети представництва його інтересів, а також консультувати клієнта щодо засобів, за допомогою яких вона буде досягнута.

2) Пункт 1.4 Типових правил передбачає, що адвокат повинен пояснити юридичний зміст справи в тому обсязі, щоб дозволити клієнту приймати обґрунтовані рішення щодо представництва своїх інтересів.

3) Пункт 3.2 Типових правил передбачає, що адвокат повинен докладати розумних зусиль для прискорення судового процесу відповідно до інтересів клієнта.

4) Пункт 2.1 Типових правил передбачає, що “адвокат повинен здійснювати незалежну професійну оцінку справи та надавати пораду, виходячи з економічних, соціальних та політичних факторів, які можуть бути пов’язані з ситуацією клієнта” [14, с. 429-430].

При чому, щодо пункту 3.2 Типових правил, деякі автори прямо зазначають, що воно чітко передбачає обов’язок адвоката інформувати клієнта про наявні альтернативи судового розгляду [14]. Щодо змісту пункту 1.2 Типових правил також було висловлено припущення, що це правило дає клієнтові право на отримання інформації про ADR [15, с. 437].

Принцип конфіденційності в межах застосування практик ADR. Право особи на отримання інформації про ADR породжує нові аспекти інформаційно-правового характеру, що постають у даних правовідносинах. Зокрема, йдеться про конфіденційність інформації, отриманої при застосуванні ADR, адже дана діяльність, на відміну від тієї ж адвокатської, не має законодавчого підґрунтя, а отже особи, що

здійснюють ADR перебувають у групі ризику щодо зловживань з боку державних органів та посадових осіб щодо інформації, отриманої в результаті даної процедури.

На прикладі медіації, в США більше ніж 250 правил конфіденційності та привілеїв, що діють в різних штатах, визначають питання про те, яка саме інформація може бути розкрита у процесі медіації без побоювання її подальшого поширення. З цією метою був розроблений однаковий закон про медіацію (The Uniform Mediation Act) [16]. Варто погодитись, що закон про медіацію та процесуальні кодекси мають закріпити гарантії того, що медіатори не можуть виступати в якості свідків в суді щодо інформації, отриманої під час медіації [17, с. 31-32].

Конфіденційність полягає у тому, що медіатор повинен тримати у таємниці і не розголошувати інформацію, яку він одержав під час спілкування зі сторонами або в процесі медіації. Крім того, він не може виступати в ролі свідка у суді щодо інформації, одержаної в процесі медіації [18, с. 104].

Відповідно до п. 2 додатку до Рекомендації № R (99) 19, прийнятої Комітетом Міністрів РЄ 15 вересня 1999 року на 679-й зустрічі представників Комітету, – “будь-які обговорення під час зустрічі мають конфіденційний характер та не можуть використовуватися в майбутньому, за винятком випадків, коли наявна згода сторін”. Відповідно до п. 30 даного додатку, “незважаючи на узгоджений принцип конфіденційності, інформація про можливу небезпеку злочинів, про яку може стати відомо під час зустрічі, передається медіатором відповідним зацікавленим особам чи органам” [19].

Повертаючись до основ відновного правосуддя, зазначимо, що основні принципи застосування програм відновного правосуддя у кримінальних справах були прийняті 2002 р. Економічною і Соціальною Радою ООН. Відповідно до них конфіденційність процесуальних дій розглядається так: “обговорення у відновних процесах, що відбуваються не публічно, мають бути конфіденційними та не можуть розголошуватися у подальшому, за винятком тих випадків, коли сторони на це погодились, або ж коли цього вимагає національне законодавство”. Інші інструменти щодо захисту прав людини також мають на меті захистити приватне життя дітей та конфіденційність процесуальних дій, де залучені діти. Вони також мають тут ураховуватися [11, с. 32].

Додаток до Рекомендації Rec (2006)8 щодо допомоги потерпілим від злочинів, прийнятої Комітетом Міністрів Ради Європи 14 червня 2006 року передбачає наступне:

1) Держави повинні вимагати від всіх юридичних осіб, включно із державними і неурядовими організаціями, які контактують із потерпілими, прийняття чітких стандартів, згідно з якими ці організації матимуть право відкривати інформацію про потерпілих третім особам при умові, коли: – потерпілий дав свою згоду на передавання такої інформації; – це вимагається за законом або є відповідне розпорядження для таких дій.

2) Щодо цих двох виняткових випадків необхідно розробити чіткі правила, які б регулювали процедуру відкриття інформації. Процедури оскарження повинні бути опубліковані на випадок ймовірного порушення правил конфіденційності [20].

В декларації про принципи Етичного кодексу у сфері відновного правосуддя зазначається, що конфіденційність як між сторонами, так і стосовно інших організацій, включаючи принцип “китайських стін” з іншою стороною тієї самої організації, що має інші функції у розгляді випадку (це потрібно для забезпечення того, щоб зміст відновних практик не руйнувався від наполегливих зусиль інтегрувати всю систему) [21, с. 35].

Висновки.

Взаємопроникнення права на правову допомогу, права на доступ до правосуддя та права на інформацію формує новий вид інформаційного права особи, що кореспондує обов'язку адвоката, а саме – право на інформацію про альтернативні види вирішення спорів (ADR). Особливо це доречно з урахуванням євроінтеграційних процесів, які сприяють розвитку правосуддя в Україні, в тому числі, в частині розвитку ADR, а також з урахуванням тенденції гуманізації кримінально-правової політики та поширенням ідеї відновного правосуддя.

Таким чином, право на інформацію про альтернативні види вирішення спорів впливає з задекларованого права на доступ до правосуддя та потребує додаткового закріплення.

Використана література

1. Про захист прав людини та основоположних свобод: Конвенція Ради Європи від 04.11.1950 р. *Урядовий кур'єр*. 17.11.10 р. № 215.
2. Жаровська І.М. Доступність права: теоретико-правові проблеми: автореф. дис. ...канд. юрид. наук: 12.00.01 / Нац. юрид. акад. ім. Я. Мудрого. Харків, 2006. 20 с.
3. Сакара Н.Ю. Проблема доступності правосуддя у цивільних справах: дис. ...канд. юрид. наук: 12.00.03 / Національна юридична академія України ім. Ярослава Мудрого. Харків, 2006. 209 с.
4. Советский гражданский процесс: учеб. / отв. ред. д-р юрид. наук, проф. М.С. Шакарян. Москва: Юрид. лит-ра, 1985. 526 с.
5. Golder v. United Kingdom, no. 4451/70, § 38, Series A no. 18. URL: <http://hudoc.echr.coe.int/eng?i=001-57496/> (дата звернення: 17.03.2019).
6. Ashingdane v. United Kingdom, no. 8275/78, § 57, Series A no. 93. URL: <http://hudoc.echr.coe.int/eng?i=001-57425> (дата звернення: 15.03.2019).
7. Ткачук О.С. Тенденції розвитку досудових процедур у цивільному судочинстві. *Часопис цивільного і кримінального судочинства*. 2016. № 4. С. 90-107.
8. Притика Ю.Д. Альтернативне вирішення спорів у сучасній процесуальній доктрині. *Правова доктрина України: у 5 т. / Н.С. Кузнецова, Є.О Харитонов, Р.А. Майданик та ін. / за заг. ред. Н.С. Кузнецової*. Харків: Право, 2013. Т. 3: Доктрина приватного права України. 758 с.
9. Спектор О.М. Альтернативні способи вирішення цивільно-правових спорів: світовий досвід та перспективи застосування у правовій системі України: монографія. Київ: Фенікс, 2013. 160 с.
10. Про вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів: Концепція від 10.05.06 р. № 361. URL: <https://zakon.rada.gov.ua/laws/show/361/2006> (дата звернення: 16.03.2019).
11. Посібник з програм відновного правосуддя. Серія посібників з кримінального правосуддя / Упр. ООН з наркотиків та злочинності. Дитячий фонд ООН (ЮНІСЕФ). URL: http://www.unicef.org/ukraine/ukr/llJvenal_Const.indd.pdf (дата звернення: 12.03.2019).
12. Estrada-Hollenbeck M. The attainment of justice through restoration, not litigation: The subjective road to reconciliation. *Reconciliation, justice and co-existence: Theory and practice*. New York and Boulder, CO and Oxford, UK: Lexington Books. 2001. P. 65-86.
13. Законопроект про медіацію обмежує права адвокатів – Олександр Дроздов. URL: <http://unba.org.ua/news/2069-zakonoprojekt-pro-mediaciju-obmezhuje-prava-advokativ-oleksandr-drozdov.html> (дата звернення: 14.03.2019).
14. Gillers, Stephen & Simon, Roy D. *Regulation of lawyers: statutes and standards*. Aspen, 1998.

15. Breger Marshall J. Should an Attorney be Required to Advise Client of ADR Options? The Catholic University of America, Columbus School of Law, 2000. URL: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.867.736&rep=rep1&type=pdf> (дата звернення: 12.03.2019).

16. Макаренко Є. Закон про медіацію: нереальна реальність. URL: <http://yur-gazeta.com/publications/practice/mizhnarodniy-arbitrazh-ta-adr/zakon-pro-mediaciyu-nerealna-realnist.html> (дата звернення: 13.03.2019).

17. Альтернативні способи вирішення спорів у контексті судової реформи в Україні. Київ, 2017. 75 с. URL: <https://www.integrites.com/wp-content/uploads/2018/07/Council-of-Europe-PUBLICATION.pdf> (дата звернення: 18.03.2019).

18. Землянська В.В. Відновне правосуддя в кримінальному процесі України: посібник. Київ: Видавець Захаренко В.О., 2008. 200 с.

19. Рекомендація Комітету Міністрів Ради Європи державам-членам, які зацікавлені в організації медіації у кримінальних справах від 15.09.1999 р. № R(99)19. URL: https://zakon.rada.gov.ua/laws/show/994_828 (дата звернення: 19.03.2019).

20. Рекомендація Rec (2006) 8 Комітету Міністрів Ради Європи державам-членам щодо допомоги потерпілим від злочинів № R (99) 19. URL: https://supreme.court.gov.ua/userfiles/Rec_2006_8_2006_06_14.pdf (дата звернення: 19.03.2019).

21. Aertsen, I., Mackay, R., Pelikan, C., Willemsens, J., and M. Wright. Rebuilding Community Connections-Mediation and Restorative Justice in Europe. Strasbourg: Council of Europe Publishing. 2004.

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

## 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.
- 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 370 грн. на рахунок Інституту.**

**Реквізити для оплати робіт:**

*Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).*

**Адреса редакції:** 01032, м. Київ, вул. Саксаганського, 110-В.

**6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net**

### **Д о у в а г и**

- Вчена рада 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

**№ 1(28)/2019**

|                                               |                                                                                                                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 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 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.                                                                                                                  |