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"

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 4(23)

2017

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 доктора і кандидата наук у галузі юридичних наук

м. Київ

УДК 002:340+316.4+338.46:002

* * * * * * * * * * *

З М І С Т

Інформаційне право

БРИЖКО В.М. Інформаційний продукт як об’єкт права власності……. **5**

ЗОЛОТАР О.О. Електронна демократія і цифрова диктатура…….. **16**

Правова інформатика

БАРАНОВ О.А. Інтернет речей (IoT): правові проблеми застосування розумних контактів……... **26**

ДОРОНІН І.М. Розвиток емерджентних (новітніх) технологій та регулювання у цій сфері як реалізація функцій держави……**41**

КАЧИНСЬКА К.А., ВАРИЧЕВА Д.І., СВИРИДЕНКО С.В. Інтернет-технології: оцінка пріоритетності маніпулювання свідомістю за допомогою методів ранжування……**49**

Інформаційна і національна безпека

ТКАЧУК Т.Ю. Забезпечення інформаційної безпеки: досвід окремих країн Східної Європи……**62**

КОПАН О.В. Дестабілізація соціально-політичної ситуації – провокація внутрішньодержавного конфлікту……**73**

БОЛДИР С.В. Перспективи реформування системи охорони державної таємниці та службової інформації…….. **79**

МАРУЩАК А.І. Питання ефективності діяльності державних органів у сфері захисту інформаційного простору України…… **86**

ЄРЕМЕНКО С.А. Організаційно-правові аспекти аналітичної роботи у сфері цивільного захисту……**93**

УХАНОВА Н.С. Захист інформаційного простору від терористичних посягань та негативних інформаційно-психологічних впливів…… **99**

Інформація в інших галузях права

РАДУТНИЙ О.Е. Штучній інтелект як суб’єкт злочину……..….. **106**

ЄВТУШЕНКО Є.В., ЛЕОНОВ Д.Б. Недійсність правочину у цивільному судочинстві…….. **116**

ОВЧІННІКОВ Р.М. Військові злочини: правове регулювання та шляхи удосконалення кримінального законодавства України…….. **122**

ГУЦАЛ І.Ю. Питання легалізації евтаназії в Україні: іноземний досвід…… **128**

До відома авторів ……..……...……..... **134**

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

Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 11.9. 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 НДІ інформатики і права
Національної академії правових наук України, протокол № 8 від 14.12.17 р.

Інформаційне право

УДК 1+340.1:338:002

БРИЖКО В.М., *доктор філософії (Ph.D.) з юридичних наук, старший науковий співробітник*

ІНФОРМАЦІЙНИЙ ПРОДУКТ ЯК ОБ’ЄКТ ПРАВА ВЛАСНОСТІ [*]

Анотація. *У статті узагальнюються деякі ключові напрацювання учених сфери інформаційного права стосовно легалізації власності у інформаційній сфері. Враховуючи розвиток та поширення новітніх технологій та їх конвергенції, формулюються пропозиції щодо внесення змін до чинного законодавства України в контексті підвищення захисту основоположних прав людини та забезпечення інтересів суспільства і держави.*

Ключові слова: *інформація, дані, інформаційні продукти, інформаційні ресурси, інформаційне суспільство, інформаційне законодавство.*

Summary. *The article summarizes key works of scientists in the area of information right related to legalization of the ownership in an information sphere. Taking into account development and expansion of the newest information technologies and their convergence, suggestions are formulated in relation to changes in the current legislation of Ukraine in the context of increasing defence of fundamental human rights and providing of society and state interests.*

Keywords: *information, data, information products, information resources, information society, information legislation.*

Аннотация*. В статье обобщаются некоторые ключевые наработки ученых сферы информационного права относительно легализации собственности в информационной сфере. Учитывая развитие и распространение новейших информационных технологий и их конвергенции, формулируются предложения относительно внесения изменений к действующему законодательству Украины в контексте повышения защиты основополагающих прав человека и обеспечения интересов общества и государства.*

Ключевые слова*: информация, данные, информационные продукты, информационные ресурсы, информационное общество, информационное законодательство.*

Постановка проблеми. Сучасною особливістю світового соціально-економічного стану є зростання значимості того, що вкладається у розуміння “інформації” в суспільних відносинах. Увага до цього слова сьогодні викликано у зв’язку широким застосуванням комп’ютерно-технологічних засобів збирання, обробки та поширення даних, що сприяє змінам у розвитку інформаційних відносин. Зазначені процеси визначають умови становлення інформаційного суспільства, сутність якого була визначена у 1993 році Комісією Європейського Союзу: “Інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою інформаційних технологій і технологій зв’язку” [1]. За цих умов пріоритетними для України постають дві проблеми: імплементація приписів європейських правових стандартів в інформаційній сфері та наукові пошуки удосконалення інформаційного законодавства.

Метою статті є деякі узагальнення проблем в інформаційній сфері та розробка пропозицій щодо удосконалення інформаційного законодавства України.

[*] Робота є продовженням фундаментальних досліджень по темі НДР “Теоретико-правові основи формування та розвитку інформаційного суспільства”.

Виклад основного матеріалу. У юриспруденції з давніх часів загальновизнано, що об’єктом права стає лише те, що є значущим для суспільства, а вирішальні критерії для наділу того або іншого явища правовим статусом в сфері соціально-економічних відносин визначаються його матеріальністю та економічною цінністю: тільки те, що може стати предметом потреби та господарського обігу, входить у сферу правового визначення таких суспільних відносин, які свідчать про наявність існування права власності на відповідний об’єкт.

Становлення інформаційного суспільства визначається розвитком та конвергенцією новітніх інформаційно-комп’ютерних технологій та мереж (про що, зокрема йдеться у [2 – 4]), основна мета застосування яких полягає в отриманні того, що стосується складу поняття “дані”. Вони при декодуванні надають все те, що пов’язане з першоосновою суспільної комунікації людини – поняттям “інформація”, яка може передбачати породження так званого “інформаційного продукту” – завершеного, з точки зору функціональної корисності у досягнутому ефекті використання результатів інформаційної діяльності, який завжди має свого автора та суб’єкта права власності.

1. *Інформація та інформаційний продукт.*

Дефініція поняття “інформація” походить від латинського “informatio”, що передбачає семантично близькі визначення: “пояснення”, “виклад”, “тлумачення”. З філософської точки зору “інформація” розглядається як віддзеркалення об’єктів матеріального світу.

Спроби зрозуміти те, що вкладається в поняття “інформація”, відомі з часів Платона. Він є родоначальником ідеї інформації – *безбарвна, безформна і невідчутна суть, по суті своїй існуюча, зрима тільки для керманича душі – розуму.* За Платоном, інформація присутня у світі об’єктивно, поза волею і бажанням людей [5]. В. Бехтерев зазначав більш конкретно – *інформація – нематеріальна субстанція у відмінності від речовини і енергії. Але вона від них невід’ємна, як від своїх носіїв. Вона виробляється, передається, сприймається, втрачається в результаті матеріальних процесів* [6]. Для Н. Вінера – *інформація – форма організації живої істоти, яка не залежить від матерії і енергії* [7]. Для А. Моля – *інформація – це кількість непередбачуваного, яка міститься в повідомленні* [8] (на наш погляд, вказане стосується “нової інформації” – *від Авт.*). Академік В. Глушков вважав, що *інформація в найширшому її розумінні є мірою неоднорідності розподілу матерії і енергії в просторі і в часі, мірою змін, які супроводжують всі процеси, що протікають в світі. ...Інформацію несуть* в собі *не тільки наповнені буквами сторінки книг або людська мова, але і сонячне світло, складки гір, шум водопаду, шелестіння листя і т.д.* [9]. За доктором юридичних наук, професором О. Гавриловим – *інформацією є дані, що використовуються, представлені у формі, придатній для передачі і обробки* [10]. Учений помічав, що до 1970-х років термін “інформація” ані в загальній теорії права, ані в галузевих юридичних науках, ані в законодавстві не застосовувався; вживали таки еквіваленти, як “дані”, “матеріали”, “відомості” та ін. [10, с. 13].

Російський словник С.І. Ожегова надає таке визначення інформації: *відомості про навколишній світ і протікаючі в ньому процеси, що сприймаються людиною або спеціальним пристроєм* [11]. Там же надано поняття “відомості”: *пізнання в будь-якій області, вісті, повідомлення, знання, уявлення про будь-що* [11, с. 698] та поняття “пізнання” – *придбання знань, збагнення закономірностей об’єктивного світу* [11, с. 546].

Українська юридична енциклопедія перекладає це слово як “роз’яснення, уявлення” [12] щодо “*документованих або публічно оголошених відомостей про події та явища, що відбуваються у суспільстві й державі та навколишньому природному*

середовищі”, яке відповідало визначенню, наданому у Законі України “Про інформацію” від 2 жовтня 1992 року № 2657-XII [13]. Що таке “документовані відомості” – Закон визначення не надавав. Виходячи з подальшого його змісту вважалось, що термін має пряме відношення тільки до “офіційного документа” – паперу, на якому розміщені відомості. У версії Закону України “Про інформацію” від 2011 р. – *інформація – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.* Крім цього, у багатьох інших офіційних документах також надавалось визначення поняття “інформація”, зокрема, щодо ДСТ України, див.[14].

Як випливає із наведеного, універсального визначення інформації не існує. Кожне з визначень вірно для певної галузі застосування, і кожне стає неконструктивним, якщо воно застосовується не за призначенням або не сприймається людиною. Дефініції у нормативних актах використовують семантичний аспект інформації, тобто змістовний опис об’єкта, предмета. “Інформація” інтерпретується як відомості, знання та ін. Подібне трактування орієнтовано на застосування документа в реальному (аналоговому) середовищі існування, утвореному мислячими суб’єктами, людьми. Лише людина може мати знання, і тільки для неї різноманітні сукупності графічних символів можуть бути “відомостями”. Тільки для людини певна сукупність символів, знаків, сигналів може інтерпретуватися як “відомості” про будь-що, а сам суб’єкт обов’язково має володіти деякою вихідною системою знань, наприклад, вміти читати. Для технічного об’єкта “інформація” не “відомості” і, тим більше, не “знання”. У неживій природі об’єкти взаємодіють з інформаційним кодом (даними), але не зі “знанням” і “відомостями”.

“Інформація” властива мислячому суб’єктові, тим самим під нею мають на увазі не лише відомості, але й їх інтерпретацію, що у наступному може забезпечувати комунікаційну взаємодію. Думка в голові людини ще не є інформацією – це прояв начитаності й інтелектуальності (творчості), що для відповідного суб’єкта в цей час є його абсолютною монополією. Те, що розуміється під “інформацією”, тільки починає виступати як предмет комунікаційної передачі. Вимовляючи слова (користуючись папером, звуком, комп’ютером, радіохвилями тощо), людина висловлює “ідею”, трансформуючи її у відомості. При цьому, людина вимовляє, доводить не думку як таку, а її копію – її форму. Виникає матеріалізація думки. Ця матеріалізація у е-просторі вже не “інформація”, а – “дані” (див. [15]), до яких інформація прикріплена, пристосована. Тільки при поєднанні ідеального і матеріального з’являються “дані”. За відсутністю одного із зазначених елементів “дані”, а разом й “інформація”, – зникають.

Що ж стосується комп’ютера – сьогодні він не може “осягнути” відомості, тобто зрозуміти їх. Це можливо лише для високоорганізованої матерії, що має складну динамічну систему управління, якою є мозок людини.

З зазначеного можна зробити висновок – “інформація” не є матеріальним об’єктом, вона – можливо віддзеркалення відомостей (знань) про дійсність в свідомості людини (причому істинне воно або помилкове – неістотне, важливо, що в свідомості). Не будучи матеріальним об’єктом, “інформація” нерозривно пов’язана з матеріальним носієм: це мозок людини або матеріально-технічні носії даних такі, як книга, диск, пристрої що запам’ятовують та ін. Іншими словами, інформація як така (тобто, взагалі кажучи, повідомлення та відомості) не може бути залучена в систему суспільних відносин без відповідного перетворення, яке фіксує її форму і спосіб подачі. Тому досить спірною є конструкція речових прав на “інформацію”, що зустрічається, – як “право власності на нематеріальне благо”, тобто наявність власності на саму “інформацію”, що просто фізично неможливе.

2. ***Інформаційний продукт як об’єкт права.*** З часів Римського права відомо розподіл будь-яких об’єктів-продуктів – “речей” всесвіту на “тілесні” і “безтілесні”.

На початку минулого століття, коли законодавство у сфері речових прав практично не зазнало змін з часів античного права, О. Шпенглер, який в часи бурхливого розвитку індустріалізації не міг уявити прихід епохи інформатизації, писав про те, що *якщо античне право було правом тіл, то сучасне право – це право функцій* [16].

У юриспруденції, як вважають сьогодні деякі дослідники, під цим розуміється не “речі”, в значенні “об’єктів” зовнішнього світу, а саме як “права” [17]. З цього приводу наголошується, що “антична думка сприймала речі як *є їх математична суть, як величини*. …Ми ж сприймаємо речі як вони *стають* і *відносяться* один до одного, як *функції*. Чому зміст патентного закону не піддається включенню в речове право? Чому авторське право не в змозі понятійно відділити духовне творіння від його форми, яку можна передавати, такої як рукопис або друкарська продукція? Чому в одній і тій же картині всупереч речовому праву доводиться розрізняти художню і матеріальну власність – за допомогою розділення *придбання оригінала* і *придбання права на відтворення*? Чому викрадання підприємницької ідеї не карається, а викрадання клаптика паперу, на якому зроблено її запис, карається в кримінальному порядку? Тому що сьогодні над нами все ще продовжує бути достатнім поняття тілесної речі: вимогою майбутнього стає перебудова всього правового мислення по аналогії з вищою фізикою і математикою”.

У наші часи власність на “річ” юридично зводиться до сукупності складових: володіння, користування і розпорядження майном. Власність на майно – це закріплене законом за суб’єктом право щодо тріади зазначених вище повноважень і, фактично кажучи, є речовим правом. Це право, на законних підставах товарно-грошових відносин, при яких товар оцінюється у грошовому еквіваленті (вартості), може бути передане іншому суб’єкту або для особистого володіння і користування (звичайно за ліцензією), або для подальшого розпорядження (за субліцензією).

Разом з тим, під суттю тілесних (майнових, матеріальних об’єктів) і безтілесних (тобто об’єктів інтелектуальної власності) “речей” можна розуміти не тільки об’єкти світу майна і внутрішнього світу людини, а – саме як юридичні права по їх використанню і захисту. І можна припускати, що для сучасного етапу інформаційного розвитку суспільства поняття “право власності” набуває іншого характеру – розширення і об’єднання в єдину наочну область. І в цьому випадку немає необхідності розуміти під “річчю” лише якусь матеріальну одиницю “майна”, що вже одержало віддзеркалення в понятті “Інтернет речей”, див. [4].

Сьогодні зарубіжні юристи серйозно обговорюють можливість визнання права власності не тільки відносно інформаційних продуктів (ресурсів), але також і відносно інших безтілесних речей-продуктів – таких, як інформаційно-комп’ютерні технології, програмне забезпечення, зміст Інтернет-сайту тощо. Більш того, як вважаємо, це стосується персональних даних, захист яких у наш час набуває нової якості, див. [18]. Важливим при цьому є те, що запровадження у міжнародному праві і більшості національних законодавств понять “приватність особистого життя”, “захист персональних даних”, “таємниця листування” та ін. свідчать про визнання того факту, що у кожної людини є її право на “власний світ”, невидима правова “територія”, яка знаходиться в її “власності” і яка проглядається в інформаційному праві як юридична реальність.

3. ***Стан справ в Україні з власністю у інформаційній сфері.***

В Україні упровадження поняття “власності” в інформаційну сферу було вперше здійснено Законом України “Про інформацію” від 02.10.92 р. № 2657-XII.

Аналіз наукових публікацій щодо проблеми застосування в законодавстві поняття “права власності на інформацію” свідчить про те, що більшість дослідників вважають за потрібне включення поняття “інформації” в економічний обіг, про це йдеться, зокрема у досить ґрунтовному, на наш погляд, дослідженні українського ученого О.І. Яременко, який справедливо зазначав (2008 р.), що “Право власності на інформацію має важливе практичне значення, перш за все для економічного розвитку держави. Поява економіки нового типу, яка отримала різноманітні назви: “інформаційна економіка”, “інформаційна індустрія”, “нова економіка”, “економіка знань”, “невагома економіка” і яка включає в себе виробництво знань, поширення інформації, створення сучасних комунікаційних систем, індустрію переробки і передачі інформації, індустрію реклами та інформаційного сервісу, довідкове та бібліотечне обслуговування, галузі, пов’язані з банківською діяльністю і страхуванням тощо, передбачає обіг інформації в комерційному обороті” [19, с. 15].

Разом з цим питання можливості “інформації” бути об’єктом власності, з точки зору традиційного розуміння речового права, тобто права власності на майно, продовжує залишатися дискусійним. При цьому, визнається, що в Україні галузева належність інформації як об’єкта права загалом, і як об’єкта права власності зокрема, визначена нечітко, а відсутність чіткого нормативного закріплення інформації в системі товарних відносин свідчить про те, що законодавство відстає від розвитку інформаційної економіки, оскільки на практиці інформація давно знаходиться в економічному обігу і є предметом цивільно-правових угод [19, с. 18, 19].

На початку 2011 року в Закон України “Про інформацію” від 02.10.92 р. були внесені зміни, які виключили з нього положення про право власності на інформацію (ст. 38) та визначення інформації товаром (ст. 39). Одночасно з тим, що протягом усього терміну дії інформаційного законодавства не існувало узгоджених визначень щодо різних галузей господарства та конкретності у механізмі реалізації цього права, сьогодні маємо більш заплутану ситуацію.

З одного боку, базовий закон 2011 р., що упорядковує інформаційні відносини в Україні, єдиним об’єктом яких є інформація, не визначає цю інформацію товаром, який має свого власника. З іншого боку, питання поставлено так, що справа власності на інформацію знаходиться у компетенції Цивільного кодексу України [20]. Основою цього є стаття 177 Кодексу, яка визначає види об’єктів цивільних прав, до яких віднесено: ***речі, у тому числі*** *гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності,* ***інформація****, а також інші матеріальні і нематеріальні блага*. Що розуміється під правом “власності”, визначає ст. 2 Закону України “Про власність” від 07.02.91 р. № 697-12: *Право власності – це врегульовані законом суспільні відносини щодо володіння, користування і розпорядження майном* [21].

Стосовно норм у редакціях Закону України “Про інформацію” та ЦКУ див. далі Таблицю.

Як зазначалось раніше, інститут майнових прав власності відомий з часів Римського права. У класичному розумінні об’єктом права власності можуть бути тільки матеріальні об’єкти, тобто “річ”, “майно”. Це визначається тріадою повноважень: володіння, користування і розпорядження майном (ст. 317 ЦКУ), хоча у рімлян цього визначення не існувало. Також у ЦКУ, у статті 179 “Поняття речі”, чітко визначено, що: *“річчю є предмет матеріального світу…”,* який *може* визначатися терміном *“товар”* (ст. 655 ЦКУ).

Таблиця.

Закон України “Про інформацію” від 02.10.92 р. **у ред. від 23.06.05 р.**	**Закон України “Про інформацію” у ред. від 13.01.11 р.**	**Цивільний кодекс України** від 16.01.03 р. у ред. від 31.05.07 р.
Стаття 38. ***Право власності на інформацію*** *– це врегульовані законом суспільні відносини щодо* ***володіння, користування і розпорядження інформацією***.	Закон не має положень, які визначають право власності на інформацію	Стаття 316. ***Правом власності є право особи на річ (майно),*** *яке вона здійснює відповідно до закону за своєю волею, незалежно від волі інших осіб*. Стаття 317. *Власникові належать права* ***володіння, користування та розпоряджання*** *своїм* ***майном***. Стаття 179. *Річчю (майном) є предмет матеріального світу, щодо якого можуть виникати цивільні права та обов’язки”*.
Стаття 39. *Інформація як товар. Інформаційна продукція … може бути об’єктом товарних відносин, що регулюються чинним цивільним та іншим законодавством*.	Закон не має положень, які визначають інформацію товаром	Стаття 658. *Право продажу товару 1. Право продажу товару, крім випадків примусового продажу та інших випадків, встановлених законом, належить власникові товару.*

До сьогодні спроби застосувати “тріаду власності на майно” до поняття “власність на інформацію”, як окремих “відомостей”, безуспішні.

Володіння. Передбачає право мати “інформацію” в незмінному вигляді. “Володіння” не може бути прирівняне до володіння річчю (майном) в значенні її фізичного володіння: передача (продаж) речі може зберігати монопольне право володіння нею, яке зникає, якщо передачі підлягає “інформація-відомості”. Тобто, *володіти “інформацією-відомостями”* без забезпечення доступу до них інших осіб неможливо, інакше виходить “знаю, але нікому не скажу” взагалі виключає юридичний сенс володіння.

Користування. Передбачає право використовувати “інформацію” в своїх інтересах. Поняття “користування” може бути застосовне до будь-якої особи, якій забезпечений доступ до “інформації-відомостей”, а не тільки для володаря права на неї. Іншими словами, *користуватися “інформацією-відомостями”* може не тільки власник (автор інформації), але і будь-яка особа, яка їх почула.

Розпорядження. Передбачає виключне право (тобто ніхто інший, окрім власника) визначати, кому “інформація” може бути надана (у володіння і користування). На відміну від матеріальних об’єктів, для “інформації” воно має інший зміст – *розпорядитися “інформацією-відомостями”* – це визначити порядок доступу до неї.

Відзначене, власне, і призвело до появи і розвитку абсолютно іншого виду прав, іменованих “інтелектуальною власністю” (у 1967 р. вона прийшла на заміну поняття “духовна власність”) [1]. Проте, ця “власність” продовжує викликати дискусії у пошуках

[1] Поняття “духовна власність” включало “промислову власність” та “авторське право” і вперше законодавчо були оформлені в Англії. Перший закон про авторські права – “Статут королеви Анни”, 1709 р. Перший патентний закон – “Статут про монополії”, 1623 р., розробив вчений, лорд-канцлер Ф. Бекон разом з юристом Е. Кохом [22, с. 134].

нового поняття, оскільки її предметом є не власність в традиційно-матеріальному розумінні, а право використання і охорони об’єкту інтелектуальної творчості.

Раніше, згідно статті 8 Закону України “Про інформацію” у ред. від 23.06.05 р. було зазначене, що *об’єктами інформаційних відносин є документована …інформація.* Сьогодні терміну “документована інформація” ми не маємо, надається лише визначення понять “документ” та “інформація” (ст. 1 Закону України “Про інформацію” у ред. від 13.01.11 р.). У сукупності ці поняття визначають – *відомості, які розміщені на носії* або *інформація, яка зафіксована.*

Поява таких електронно-структурних об’єктів як “веб-сайт”, “веб-документ”, “веб-сторінка” є свідченням того, що поняття “інформація, яка зафіксована” взагалі засноване на двоєдності відомостей та будь-якого матеріального носія, на який вона заноситься у вигляді символів, букв, е-сигналів, е-структур тощо. У результаті цього відбувається матеріалізація інформації та виникає об’єкт права власності – “інформаційний продукт”. Цей інформаційний продукт є об’єктом правовідносин як для матеріального середовища: книжка, журнал, стаття та ін., так і для віртуального середовища: банк даних, веб-сайт, веб-сторінка, доменне ім’я і ін.

Таким чином, “інформація” за певних умов може бути матеріалізована у вигляді об’єкту під назвою “інформаційний продукт”, що дає підставу, у такому разі, віднести його до категорії “речей”. Тобто, на “інформаційній об’єкт, який зафіксований” (матеріалізований людиною) однозначно розповсюджується право “речової” (“майнової”) власності. Й тільки у такому разі регуляція інформаційних відносин може бути віднесена до компетенції ЦКУ, головне завдання якого – регулювання майнових відносин.

Однак, назва Глави 15 ЦКУ “Нематеріальні блага” спрямовує на те, що “інформація” (ст. 200) та “інтелектуальна власність” (ст. 199) є нематеріальними благами. Ст. 419 ЦКУ взагалі визначає те, що існують два види власності: *право інтелектуальної власності* та *право власності на річ, які не залежать одне від одного.* Враховуючи також викладене у статті 179 ЦКУ *(“річчю” є предмет матеріального світу*), можна дійти остаточного висновку – “інформація” та “інтелектуальна власність” в Україні не є “речами” (“майном”, “товаром”). Проте раніше, у ст. 177 ЦКУ, майнові та немайнові блага були зведені “докупи”: “***об’єктами цивільних прав є речі****, у тому числі …****інформація****…”.*

Український вчений О.О. Баранов, зазначає в [23], що законодавець у ЦКУ не визначив в якості якого предмету матеріального світу може бути представлена інформація. Використовуючи норми ЦКУ, неможливо логічно замкнути зв’язок: “інформація-річ-право майнової власності”. Таким чином, відповідно до ЦКУ, “інформація” не може бути об’єктом права власності.

Одночасно, ЦКУ також містить норми, які свідчать про протилежне. У статті 303 ЦКУ вказано, що *Особисті папери (документи, фотографії, щоденники, інші записи, особисті архівні матеріали тощо) фізичної особи є її власністю*. Відповідно до статті 178 ЦКУ об’єкти цивільних прав, в тому числі й інформація, можуть вільно відчужуватися або переходити від однієї особи до іншої в порядку правонаступництва чи спадкування або іншим чином, якщо вони не вилучені з цивільного обігу. Законодавець у статті 969 ЦКУ визнає документи, як окрему форму інформації, в якості цінностей, які можуть бути передані до банку на зберігання. Більш того, у статті 1010 ЦКУ до майна довірителя відносяться його документи. Відповідно до Глави 62 ЦКУ: *До результатів виконання науково-дослідних або дослідно-конструкторських та технологічних робіт, які має право використовувати замовник, відносяться наукові дослідження та конструкторська документація, в якості конкретних організаційних форм інформації.*

В умовах ринкових відносин, у яких застосовують інформаційні технології, різні види інформаційних продуктів дедалі більше перетворюються на високоліквідний товар, тобто предмет майнових відносин. Збільшення доданої вартості в економіці відбувається значною мірою за рахунок інформаційно-інтелектуальних пошуків, обробки і підвищення інформаційно-технологічного рівня обігу різних інформаційних продуктів. Ці продукти перетворюються на найбільш цінний ресурс, як один з основних товарів, сумарна вартість якого неухильно наближається до загальної вартості продуктів матеріального світу.

Відомий фахівець у сфері інформаційного права, доктор юридичних наук І.Л. Бачило, визнає інформаційний об’єкт предметом “комплексного правового регулювання”, зокрема за допомогою права інтелектуальної власності і майнового права. Інформацію, яка розміщена на носієві (“документована інформація”), вона вважає предметом матеріального світу, тобто відносить до категорії речей і поширює на неї право речової власності [24]. Вважаємо, у відзначеному аспекті йдеться лише про “справжню документовану інформацію”, а не про підроблений або незаконно запозичений документ.

На превеликий жаль, чинне нормативно-правове впорядкування економічного обігу інформаційних продуктів продовжує бути суперечливим і не має правового механізму регулювання товарно-грошових відносин, пов’язаних з власністю на них. У методологічному аспекті, стосовно обчислення вартості інформаційних продуктів, деякі напрацювання є (див., наприклад [25, с. 71-81, 103-130]), але їх недостатньо, оскільки продовжує існувати потреба у подальших наукових дослідженнях і вирішенні ще багатьох питань [2. Як вважаємо, зазначене суттєво гальмує розвиток системи правового упорядкування суспільних відносин в інформаційній сфері та процес введення інформаційних продуктів в господарський обіг, що негативно відбивається на вирішенні питань захисту прав суб’єктів інформаційних відносин.

Висновки.

1. Універсальної дефініції поняття “інформація” не існує. Інформація як філософсько-наукова категорія разом з поняттями матерії і енергії не підлягає науковому визначенню. За гіпотетичним припущенням, інформація – це не “віддзеркалення дійсності”, не “результат вибору”, не “засіб вивчення реальності” тощо, а – це так званий “движитель” (рушійна сила, за Платоном – “ідеальний початок”) появи, протікання та припинення процесів роботи так званого “двигуна” (“приймача”), який надає рух у часі і просторі та визначає усі зміни, перетворення, знищення тощо у Всесвіті. Вказані раніше визначення є наслідком проміжного впливу на будь-який “приймач” зазначеного “движителя” та уявлення людини про те, що він надає. Якщо, для прикладу, біологічний організм розглядати умовно як “двигун” життя, то кров як форма “движителю” містить в собі те, що підтримує його роботу. І це щось є не тільки випадкова, а й слушна компіляція біоатомів-генів, на якій записана генетична інформація, що визначає вроджені якості. Головне те, що інформаційне наповнення та інформаційна взаємодія завдяки відповідному розташуванню генів один біля одного надають можливість для подальшого життя у відповідній формі. За аналогією те ж саме стосується й будь яких об’єктів

[2] Німецький патентознавець Г. Штумпф (1988 р.) відзначав: “Навіть не повний перелік істотних для визначення ліцензійної винагороди (на інформаційній продукт – *від. Авт.*) чинників показує, що розрахунок вартості ліцензії по твердій формулі неможливий. Дуже складний не тільки розрахунок окремих чинників, але і визначення їх взаємозв’язків” [26]. Сьогодні у торгівлі інформаційними продуктами прагнуть мати хоча б приблизну цифру їх вартості, порядок яких можуть підказати спрощені формули або міжнародні прецеденти вартості схожих інформаційних об’єктів окремих галузей. Останнє значно спрощує економічні розрахунки, одночасно дозволяючи точніше і орієнтуватися в кон’юнктурі та потребах ринку.

Всесвіту. При отриманні або втраті (зміні) його інформаційного наповнення матеріальний об’єкт може змінюватися, трансформуватися або зникати. У науковому аспекті поняття “інформації” знаходиться за межами фізичних уявлень (метафізики), екзистенціоналізму (пошуки, що пов’язані з правом та законом, свободою та свавіллям) та трансцедентності, яка оперує неможливістю пізнання, для прикладу, Бога, душі, смерті, часу.

Для людини окрема “інформація” – це лише повідомлення або відомості, які можуть зменшувати (або не зменшувати) не знання у її одержувача, а її предметна сукупність може свідчити (або не свідчити) про появу інформаційного продукту.

2. З юридичної точки зору, запровадження категорії “власність на результати інформаційної діяльності” можливо за умови застосування в інформаційному законодавстві не поняття *“власність на інформацію”*, а застосування поняття ***“власність на інформаційний продукт”***, яке у обсяг логічного кола інформаційних ознак (повідомлення, відомості та дані) може включати такі інформаційні об’єкти як “інформаційні технології” та “інформаційні послуги”, а також – окрему “інформацію-відомості”, кожен з яких має завершений в створенні та корисний у використанні зміст.

У застосуванні дефініції “інформаційного продукту”, як об’єкту правовідносин, важливим є аспект, пов’язаний з його юридичним захистом, що передбачає наявність функціонально завершеного для використання рішення інформаційного завдання (проблеми) для задоволення потреб у будь-якій галузі господарства, соціально-культурного розвитку та захисту інтересів людини, суспільства та держави, а також – наявність критеріїв, за якими “інформаційний продукт” може бути визначений.

Основними критеріями, які можуть юридично визначати наявність ***“інформаційного продукту”*** є: “організаційно-функціональна форма його матеріального втілення”; “завершеність для використання”; “корисність у забезпеченні задоволення інформаційних потреб суб’єктів”. Для співставлення з критеріями, які діють у сфері інтелектуальної власності (у патентному праві) зазначимо, що основними критеріями в отриманні охоронного документа-інформації по патенту є: “світова новизна”; “винахідницький рівень”; “технічне рішення завдання”; “позитивний ефект” [27].

Запровадження поняття “інформаційний продукт” у законодавство, як *основного об’єкта права власності в інформаційній сфері*, у принципі дозволяє поширити правове регулювання на результати інформаційної діяльність і упорядкування товарно-грошових відносин різних суб’єктів. Головне – правильно визначатися з тим, який суб’єкт є власником інформаційного продукта, який – володільцем, який – користувачем, а який одержує згідно закону і договору статус розпорядника.

Як вважаємо, в сферу інформаційного права має бути введений принцип товарності. Тобто, “інформаційний продукт”, який розміщений на матеріальному носії, відповідає основним його критеріям і передбачає забезпечення потреб в упорядкуванні товарно-грошових відносин, має одержати статус товару, на визначених законом умовах.

3. Вважаємо за необхідне здійснити внесення змін до чинного Закону України “Про інформацію”, в основу яких можуть бути покладені такі основні складові:

1) додаткове визначення понятійно-категоріального апарату:

Інформаційна діяльність – будь-які дії, пов’язані з інформацією (відомостями, даними) та інформаційними продуктами (інформаційними технологіями, інформаційними ресурсами та інформаційними послугами [3]) суб’єктів інформаційних відносин.

[3] Згідно зі статтею 1 Закону України “Про Національну програму інформатизації”: “інформаційна послуга – дії суб’єктів щодо забезпечення споживачів інформаційними продуктами”.

Інформаційний продукт – результат розумової (інтелектуальної) або техніко-технологічної діяльності в інформаційній сфері, який має завершену для використання організаційно-функціональну форму матеріального втілення (книги, документи, фільми, інформаційні технології, інформаційні ресурси, бази даних, сайти) та призначений для задоволення потреб суб’єктів інформаційних відносин.

Інформаційний ресурс – сукупність інформаційних продуктів певного призначення, (у тому числі інформаційних технологій, реєстрів, баз даних, сайтів) необхідних для забезпечення інформаційних потреб суб’єктів інформаційних відносин.

Право власності на інформаційний продукт – врегульовані законодавством суспільні відносини щодо володіння, користування і розпорядження ним;

2) врегулювання питань власності на інформаційні продукти:

1. Інформаційні продукти є об’єктом права власності фізичних і юридичних осіб або держави. Інформаційні продукти можуть бути об’єктом права власності у повному обсязі та об’єктом володіння, користування чи розпорядження.

Власник інформаційного продукту щодо об’єкта своєї власності має право здійснювати будь-які законні дії.

2. Підставами виникнення права власності на інформаційний продукт є:

створення інформації своїми силами і за свій рахунок;

договір на створення інформації;

договір, що містить умови переходу права власності на інформаційний продукт до іншої особи.

3. Інформаційні продукти, створені кількома фізичними або юридичними особами, є колективною власністю її творців. Порядок і правила користування такою власністю визначаються договором, укладеним між співвласниками.

Інформаційні продукти, створені юридичними особами або придбані ними іншим законним способом, є власністю цих осіб.

Інформаційні продукти, створені за кошти державного бюджету, є державною власністю. Інформаційні продукти, створені на правах індивідуальної власності, можуть бути віднесені до державної власності у разі її передачі на зберігання у відповідні бази даних, реєстри, фонди або архіви на договірній основі.

4. Власник інформаційного продукту має право призначати особу, яка здійснює володіння, використання і розпорядження інформацією, та визначати правила обробки інформації і доступу до неї, а також встановлювати інші умови щодо інформації.

5. Персональні дані фізичних осіб є об’єктом права приватної власності цих осіб. Порядок обігу персональних даних визначається законодавством.

6. Інформаційні продукти можуть бути об’єктами товарних відносин відповідно до законодавства.

7. Ціни і ціноутворення на інформаційні продукти встановлюються відповідно до законодавства.

Використана література

1. Пилипчук В.Г., Брижко В.М. Проблеми становлення і розвитку інформаційного законодавства в контексті євроінтеграції України // Інформація і право. – № 1(1)/2011. – С. 11.

2. Брижко В. Приватність даних у хмарних технологіях // Інформація і право. – № 4(19) / 2016. – С. 47-59.

3. БрижкоВ. Конвергенція новітніх технологій : стан і перспективи змін у інформаційних відносинах / В. Брижко, В. Фурашев // Інформація і право. – № 1(20)/2017. – С. 51-67.

4. Баранов О. Захист персональних даних в сфері Інтернет речей / О. Баранов, В. Брижко // Інформація і право. – № 2(17)/2016. – С. 75-81.

5. Платон : соч. в 3-х т. ; [пер. с древнегреч. ; под ред. А.Ф. Лосева и В.М. Асмуса]. – М. : “Мысль”, 1968.

6. Брижко В. До гносеології категорії “інформація” // Інформація і право. – № 2(2)/2011. – С. 13.

7. Винер Н. Кибернетика и общество / Н. Винер. – М., 1958.

8. Моль А. Теория информации и эстетическое восприятие / А. Моль. – М., 1966.

9. Глушков В.М. Мышление и кибернетика / В.М. Глушков // Вопросы философии. – 1963. – № 1. – С. 34.

10. Гаврилов О.А. Курс правовой информатики : учебник для вузов / О.А. Гаврилов. – М. : Издательство “НОРМА”, 2000. – 432 с.

11. Ожегов С.И. Словарь русского языка / С.И. Ожегов. – М. : Изд. “Русский язык”, 1989. – С. 253.

12. Юридична енциклопедія : в 6 т. ; редкол. Ю.С. Шемчученко (голова редкол.) та ін. – К. : “Укр. енцикл.”, 1998. Т. 2: Д–И. – С. 717.

13. Про інформацію : Закон України від 02.10.92 р. № 2657-XII. – Режим доступу : //www.rada.gov.ua

14. Інформаційне суспільство. Дефініції : людина, її права, інформація, інформатика, інформатизація, телекомунікації, інтелектуальна власність, ліцензування, сертифікація, економіка, ринок, юриспруденція / [В. Брижко, О. Гальченко, О. Орєхов, А. Чорнобров] ; за ред. д.е.н., професора М.Я. Швец. – К. : “Інтеграл”, 2002 р. – 220 арк. – С. 88.

15. Брижко В. До питання застосування у правотворчості понять “інформація” та “дані” // Правова інформатика. – 2005. – № 4(8). – С. 31-37.

16. Шпенглер О.Ш. Закат Европы / О.Ш. Шпенглер : [пер. с нем. под ред. А.А. Франковского]. – М., 1998. – Режим доступу : http://az.lib.ru/s/shpengler_o/text_1922_zakat_evropy.shtml

17. Право собственности – история и современность. – Режим доступу : http://www.pravo.vuzlib.su/book_z021_page_10.html

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

19. Яременко О.І. Інформація як об’єкт права власності в Україні // Правова інформатика, № 4(20) / 2008. – С. 15.

20. Цивільний кодекс України : Закон України від 16.01.03 р. № 435-IV ; у ред. від 31.05.07 р. // Відомості Верховної Ради України. – 2003. – №№ 40-44.

21. Про власність : Закон України від 07.02.91 р. № 697-12. – Режим доступу : //www.rada.gov.ua

22. Брижко В. е-майбутнє та інформаційне право / В. Брижко , Ю. Базанов, М. Швець ; за ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – [2-е вид., доп.]. – К. : НДЦПІ АПрН України. – 2006. – 233 с.

23. Баранов О. Право власності на інформацію // Правова інформатика. – 2008. – № 1(17). – С. 15-19.

24. Бачило И.Л. Функции органов управления / И.Л. Бачило. – М., 2005. – С. 71-74.

25. Брижко В.М. Ліцензування прав на інформаційні ресурси / В.М. Брижко, Ю.К. Базанов, Л.С. Харченко. – К. : Національне агентство з питань інформатизації при Президентові України, 1997 р. – 132 с.

26. Штупф Р. Лицензионній договор / Р. Штупф . – М. : “Прогресс”, 1988 г.

27. Брижко В. Патентознавство як самостійна наукова дисципліна / В. Брижко. – (Національне агентство з питань інформатизації при Президентові України). – К., “Інтеграл”,1996 г. – 184 с.

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

УДК 342.3(308)

ЗОЛОТАР О.О., *кандидат юридичних наук, старший науковий співробітник,*
НДІ інформатики і права НАПрН України

ЕЛЕКТРОННА ДЕМОКРАТІЯ І ЦИФРОВА ДИКТАТУРА

Анотація. *Досліджується використання інформаційно-комунікаційних технологій в інтересах політичного режиму та його соціально-правові наслідки.*

Ключові слова*: інформаційне суспільство, електронна демократія, цифрова диктатура, Україна, Європа, Китай.*

Summary*. The use of information and communication technologies in the interests of the political regime and its social and legal consequences are researched.*

Keywords*: information society, e-democracy, digital dictatorship, Ukraine, Europe, China.*

Аннотация*. Исследуется использование информационно-коммуникационных технологий в интересах политического режима и социально-правовые последствия такового.*

Ключевые слова*: информационное общество, электронная демократия, цифровая диктатура, Украина, Европа, Китай.*

Постановка проблеми. У сучасному світі прикметники “цифровий” і “електронний” вживаються для характеристики різних соціально-правових явищ, що пов’язані з використанням інформаційних технологій. На сьогодні у побутовому, медійному, науковому і політико-правовому вжитку зайняли важливе місце такі категорії як “електронний уряд”, “електронна демократія”, “електронні гроші”, “цифровий підпис”, “цифрові права”, “цифрові загрози”, “електронний уряд”, “цифризація” тощо. Всі ці терміни “породили” інформаційне суспільство, щодо самого факту існування якого ведеться запекла дискусія на науковому і політичному рівні, але дійсність неминуче свідчить про зміну етапу історичного розвитку людства, якому властивим було домінування промислового виробництва, на новий – де основним виробничим ресурсом стає інформація, а основними засобами виробництва і управління – інформаційно-комунікаційні технології.

“Інформаційне суспільство”, як категорія, пройшло шлях осмислення від футурологічної і соціологічної концепцій до закріплення на державному рівні – як “одного з головних пріоритетів України” [1] і на міжнародному рівні – як можливості сягнення “економічних, соціальних і культурних переваг” [2] для людства в цілому.

Результати аналізу наукових публікацій. Теоретики інформаційного суспільства (в різноманітності його назв) Ю. Хаяші, Й. Масуда, Д. Бел, М. Кастельс, Ф. Махлуп, П. Друкер та інші, одностайно відзначали неминучість змін в політичній організації суспільства, оскільки свобода інформації безпосередньо впливає на політичний процес. Зокрема, Й. Масуда визначав серед основоположних рис інформаційного суспільстваті, що “в інформаційному суспільстві основним суб’єктом соціальної активності стане “вільна громада” [3, с. 38]. Водночас, критики концепції інформаційного суспільства, зокрема Ф. Уебстер та К. Мей, вважають, що інформаційні технології – це позасоціальний феномен, тому вони не можуть змінити фундаментальних засад існування суспільства.

В цій статті автор робить наукову розвідку щодо використання інформаційно-комунікаційних технологій в інтересах політичного режиму та соціально-правових наслідків інтегрування інформаційно-комунікаційних технологій в політичну діяльність.

Дослідження опирається на праці з теорії держави і права, адміністративного та інформаційного права, а також праці філософів, соціологів, політологів та фахівців з безпеки, що досліджували питання, дотичні до предмету вивчення. Емпіричну базу дослідження становлять міжнародні та національні правові акти, статистичні дані, а також інформація щодо соціальних процесів, що опублікована в українських та зарубіжних інформаційних виданнях.

Метою статті є узагальнення поглядів щодо використання інформаційно-комунікаційних технологій в інтересах політичного режиму та його соціально-правові наслідки.

Виклад основного матеріалу.

Електронна демократія. Українські науковці відзначають існування “певних етапів інформатизації: електронізація, комп’ютеризація, медіатизація і, нарешті, інтелектуалізація – процес розвитку здатності суспільства до породження і сприйняття знань, тобто підвищення інтелектуального потенціалу, включаючи використання засобів штучного інтелекту. Таким чином, основною ціллю соціальної інформатизації є побудова інтелектуального суспільства – суспільства, побудованого на знаннях” [4, с. 14].

В сучасному законодавстві, на думку вже згаданих вчених, методологічно невірно використовувати та популяризувати термін “електронний” – електронна демократія, електронна економіка, електронна комерція, електронна послуга, електронна культура, електронна освіта, електронна медицина. Це мовне запозичення не єдине, поруч з ним увійшли “цифровізація” (диджіталізація, дигітилізація), і його похідні – цифрова демократія [5], цифровий підпис, цифрові права, а також “кібер-” – кібердемократія [6; 7], кібербезпека, кіберпростір, кіберзлочини тощо.

Тим не менш, категорії “електронна демократія”, “електронна комерція”, “електронна послуга” та ін. міцно вкоренилась в науковій і політико-правовій лексиці, про що свідчить їх використання в соціальних, політичних, правових науках, а також в міжнародному праві та законодавстві переважної кількості розвинених країн. Більш того, термін-прикметник “електронний” часто замінюється його англомовним аналогом – префіксом “е-”: е-демократія, е-голосування, е-комерція, е-послуга, е-освіта, е-медицина тощо [8, с. 5, 96-115].

Що ж саме відрізняє електронну демократію від демократії “доцифрового” суспільства? Електронна демократія передбачає участь громадян у управлінні державою на всіх рівнях (від органів державної влади і місцевого самоврядування до самоорганізації населення) за допомогою інформаційно-комунікаційних інструментів. Водночас, е-демократія не може розглядатись як окрема політика поза політикою демократизації як такої. Разом з тим вона спроможна суттєво посилити та прискорити демократичні процеси у всіх сферах державного життя.

У навчальному посібнику з електронної демократії Н.В. Грицяк та С.Г. Соловйов визначають два підходи до її розуміння: у вузькому розумінні мають на увазі застосування ІКТ для забезпечення (електронного супроводу) прав громадян; а е-демократія у широкому розумінні передбачає залучення громади за допомогою сучасних інформаційних технологій до вирішення різноманітних суспільно-політичних завдань [9, с. 5].

Довший час в Україні ототожнювали е-демократію і е-урядування, при чому акценти розставлялись на користь останнього. Вже згадуваний Закон України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” не містив поняття електронної демократії. Основні засади та напрями розвитку е-демократії донедавна визначались Концепцією розвитку електронного урядування в

Україні [10], Стратегією державної політики сприяння розвитку громадянського суспільства в Україні [11], та Планом дій з впровадження в Україні ініціативи “Партнерство “Відкритий Уряд” [12]. Проте, в листопаді 2017 року нарешті Кабінет Міністрів України схвалив Концепцію розвитку електронної демократії до 2020 року та План заходів щодо її реалізації до кінця 2018 року [13], розроблені Державним агентством з питань електронного урядування України спільно з Коаліцією розвитку електронної демократії. Затверджений план заходів передбачає формування нормативно-правового забезпечення розвитку електронної демократії. А це означає створення нормативно-правових засад для забезпечення належного функціонування електронних інформаційних ресурсів органів влади; вдосконалення механізму подання та розгляду електронних петицій; підвищення участі громадян у процесах прийняття рішень через запровадження інструменту електронних консультацій; формування основи для забезпечення електронного голосування та удосконалення принципів розвитку відкритих даних.

Світовий досвід із впровадження інструментів е-демократії свідчить про розуміння е-демократії як складової електронного урядування поруч із постачанням е-публічних послуг. Такого висновку можна дійти на підставі аналізу Рекомендації Комітету Міністрів країн-членів Ради Європи щодо е-урядування [14], яка визначає е-демократію як використання ІКТ в демократичних процесах, яке дозволяє: (1) посилити участь, ініціативність та залучення громадян на національному, регіональному та місцевому рівнях публічного життя, (2) покращити прозорість демократичного процесу прийняття рішень, а також підзвітність демократичних інститутів, (3) покращити чутливість/ зворотну реакцію органів влади на звернення громадян, (4) сприяння публічним дебатам та увагу громадян до процесу прийняття рішень.

В Рекомендаціях Ради Європи щодо електронної демократії (Recommendation CM/Rec(2009)1 [15] визначено 20 принципів е-демократії, серед яких:

- основне завдання електронної підтримки демократії – це посилення демократії, демократичних інститутів та процесів, поширення демократичних цінностей;
- е-демократія повинна бути сумісна та пов’язана із традиційними процесами демократії. Кожен процес демократії (електронний чи традиційний) відграє свою роль і не може застосовуватись як універсальний;
- е-демократія спирається на демократичні, гуманістичні, соціальні, етичні та культурні цінності суспільства, в якому вона запроваджується;
- е-демократія тісно пов’язана із “добрим урядуванням”, тобто здійснення влади у електронній формі повинно спиратись на принципи результативності, ефективності, участі, прозорості, підзвітності;
- е-демократія повинна підтримувати та впроваджувати фундаментальні свободи, права людини, включаючи свободу доступу до інформації;
- всі заінтересовані сторони е-демократії повинні включатись у демократичні процеси та отримувати вигоди від такої участі;
- е-демократія стосується багатьох різноманітних груп стейкхолдерів (заінтересованих сторін) і потребує їх співпраці. У формування та впровадження е-демократії повинні включатись не тільки органи публічної влади, але й громадяни, інститути громадянського суспільства, політики та політичні інституції, медіа та бізнес-спільнота;

- кожен тип участі у політиці може бути досягнений через е-демократію Йдеться про (1) постачання інформації, (2) комунікацію, консультацію, обговорення, (3) угоди, уповноважена участь, спільні рішення, прийняття рішень;
- е-демократія є пов’язана із певним типом демократії і може впроваджуватись в системах різного рівня складності, рівня розвитку демократії, різних типів демократії;
- особливо, е-демократія через сучасні ІКТ приваблює молодь до демократії, демократичних інститутів, демократичних процесів;
- недержавні організації можуть як використовувати е-демократію у своїх інтересах, так і здійснювати контроль за здійсненням е-демократії в інтересах громадян;
- публічна влада виграє від дискусій та ініціатив, які стосуються е-демократії та розвиваються у середовищі громадянського суспільства;
- цілі е-демократії подібні до цілей “доброго врядування”: прозорість, підзвітність, включення (інклюзія), доступність, участь, сталий розвиток, довіра до демократії, демократичних інститутів, демократичних процесів, соціальна згуртованість;
- е-демократія відкриває можливості участі у політиці вразливих категорій громадян, які не мають можливості впливу на публічні рішення, і голос яких як правило, ігнорується;
- медіа відграють вирішальну роль в е-демократії і спроможні створити форум для публічних дебатів, на яких громадяни можуть заявити про свої інтереси;
- новітні медіа та провайдери е-послуг спроможні покращити доступ громадян до інформації та сформувати кращу базу для участі громадян у демократичних процесах;
- е-демократія є інтегральною частиною інформаційного суспільства, яка постачає інноваційні інструменти участі громадян у публічному житті та політичних процесах;
- е-демократія базується на наступних поняттях: (1) активне постачання комплексної, збалансованої, об’єктивної інформації, яка дозволяє чітко зрозуміти суть публічних проблем, альтернатив, можливостей, рішень в політиці. Цей концепт інформації чітко пов’язаний із свободою інформації та свободою слова, (2) широке розуміння громадянства, яке включає осіб та групи осіб, які постійно проживають на території держави, включені у політичні організації безвідносно національності, (3) участь громадян – залучення до вирішення публічних справ осіб та груп осіб, (групи інтересів, корпорації/професійні об’єднання, асоціації, неприбуткові організації). Така участь повинна гарантувати вплив на демократичний процес, можливість удосконалення якості та прийнятності результатів демократичного процесу, (4) уповноваження та посилення спроможності – засоби підтримки права громадян на державне управління, надання громадянам ресурсів та повноважень для участі у політиці, (5) включення (інклюзія) – політичне та технологічне посилення спроможності громадян до участі у політиці, (6) обговорення – раціональні дебати серед рівних, на яких люди відкрито дискутують, підтримують чи критикують інші точки зору;
- е-демократія дозволяє брати участь у демократичних процесах будь-якій заінтересованій стороні безвідносно місцезнаходження;
- е-демократія об’єднує виробників політики та громадян у нову форму взаємодії та прийняття рішень, за якої стає максимально доступною інформація про думку громадськості, потреби, очікування та інтереси громадян.

В Рекомендаціях Ради Європи визначаються наступні сектори чи напрямки е-демократії: (1) е-парламент, (2) е-законотворення, (3) е-голосування, (4) е-правосуддя, (5) е-медіація (досудове вирішення спорів), (6) е-навколишнє середовище (екологія),

(7) е-вибори, (8) е-референдум, (9) е-ініціативи, (10) е-голосування, (11) е-консультації, (12) е-петиції, (13) е-політичні компанії, (14) е-опитування.

Що цікаво, в європейських державах опублікування інформації електронними засобами як вид діяльності відноситься до е-послуг, і вважається необхідною умовою забезпечення участі громадян в управлінні державою та реалізації їх законних прав та свобод. В Україні ж часами надзвичайно складно добитись від державних органів оприлюднення публічної інформації. Окрім того, великими проблемами на шляху до впровадження нових цифрових інструментів стоїть не лише корупція, а й популізм, коли велика частина людей вважає себе компетентними, не маючи потрібних знань і досвіду. Тому ознайомлення з відкритими даними і правильність їх використання займає дуже важливе місце у розвитку демократії, зокрема і електронної, в Україні [16].

При цьому важливим є усвідомлення як владою, так і самим суспільством того факту, що роль технологій в е-демократії не є визначальною. Велика кількість та якість технологій не зумовлюють якість демократичного процесу. Відповідальність за впровадження технологій повинна лежати на інституції, яка відповідає за е-демократію як політику. Про це свідчить досвід багатьох розвинених країн, де вже довший час використовуються інструменти е-демократії – Естонії, Сполученого Королівства, Німеччини, Швеції та інших.

Цифрова диктатура. Про небезпеку, що “ми рухаємося у напрямі контрольованого суспільства”, попереджав ще Й. Масуда в своїй праці “Комп’ютопія”. Він писав про сувору альтернативу, що стоїть перед людством – вибором між “двома різко контрастуючими моделями майбутнього”: між “Комп’ютопією”, тобто справді демократичним, правовим інформаційним суспільством, та “автоматизованою державою”. Професор шукав пояснення в історії виникнення технологій, адже впродовж перших років комп’ютери (а потім і мережі) використовувалися, в першу чергу, військовими, безпековим сектором та іншими урядовими структурами. Водночас, така ситуація, на його думку, загрожувала “зазіханням на індивідуальну самотність та кризою підконтрольності...” [3, с. 39]

І найстрашніші прогнози футуролога мають шанс реалізуватись в сучасному Китаї.

14 червня 2014 року Державна рада Китаю опублікувала документ під назвою “Проект плану зі створення системи соціального кредиту довіри, 2014 – 2020 рр.”) [17], метою якого стане формування рейтингу благонадійності жителів КНР.

Передумови для формування систем соціального контролю були закладені в 2007 році, коли були опубліковані “Деякі зауваження канцелярії Держсекретаря КНР про створення системи соціального кредитування” [18]. Тоді в проекті за основу було взято систему скорингу – оцінки платоспроможності, яка є поширеною світовою практикою. Мета, яка декларувалась в цьому документі – “використання міжнародного досвіду, вдосконалення системи сканування щодо кредитування, оподаткування, виконання контрактів, якості продукції”.

Але в документі 2014 року було змінено не лише суб’єктний склад – з компаній на громадян Китаю і всіх мешканців, а й підходи та цілі реалізації програми. Система “соціального кредиту довіри” передбачає відстежування і оцінку поведінки людей. Та формування в режимі реального часу рейтингу довіри, який буде прив’язаний до внутрішнього паспорту і буде знаходитись у вільному доступі в централізованій базі даних в Інтернеті.

В тестовому режимі систему було впроваджено приблизно в тридцяти містах Китаю, зокрема в місті Жунчен в провінції Шаньдун. Всім жителям міста (670 тисяч осіб) було надано вихідний рейтинг 1000 балів. Далі в залежності від їх поведінки рейтинг або

зростає, або падає. Розрізнена інформація про життя і діяльність громадянина надходить з муніципальних, комерційних, правоохоронних, судових органів в єдиний інформаційний центр, де обробляється за допомогою технології “Великі Дані” (англ. – Big Data). В цілому рейтинг формується на основі аналізу 160 тисяч різних параметрів з 142 установ. Передбачено преміювання за доноси – громадянину, що повідомив куди слід про “не доброчесні” дії свого сусіда, додається як мінімум п’ять балів [19].

Над впровадженням цієї системи працювали китайські корпорації, зокрема, компанія China Rapid Finance – партнера Tencent, котра розробила месенджер WeChat з базою в понад 850 млн користувачів [19]. Активно сприяє системі торгівельний Інтернент-гігант Alibaba, яким в Китаї користуються більше половини Інтернет-користувачів. Рейтингова система Alibaba, яка називається Sesame Credit, вже другий рік нараховує користувачам бали виходячи з їх споживчої поведінки.

Sesame ранжує клієнтів за шкалою від 350 до 950 балів. Починаючи з 600 балів користувач має право на кредит без застави на $ 800 для покупок он-лайн, з 650 – може орендувати машину теж без застави, з 700 – експрес-оформлення дозволу на поїздки в Сінгапур, та інші переваги [20]. Дані цієї корпорації зараз стали прототипом формування майбутнього “Соціального рейтингу”. Дочірня компанія через систему AliPay, а також також каршеринговий сервіс Didi Chuxing (конкурент Uber в Китаї) та і сервіс для знайомств Baihe вже включились в співпрацю.

Журналісти The Wall Street Journal досліджували, як формується рейтинг, і акцентували увагу на 5 складових – кредитній історії, виконавчій дисципліні, персональних даних, поведінці і відносинах. Якщо перші два були властиві і вже згадуваним системам скорингу, то три останніх вважаються правопорушеннями у демократичних країнах. Адже, крім кредитної історії, в традиційному розумінні Sesame враховує, чим людина займається в мережі, на підставі дослідження персональних даних користувача: “Якщо хтось, наприклад, по 10 годин на день грає у відеоігри, то він нероба, а якщо людина часто купує підгузки, то, швидше за все, це батько, а значить, в цілому має почуття відповідальності” [21]. Активних гравців Alibaba вираховує завдяки чемпіонатам з Dota 1, Counter-Strike, StarCraft 2, Hearthstone [20].

Аналізу підлягають і стосунки людини, адже, якщо хтось із знайомих (друзів у соцмережах) напише в інтернеті коментар, що негативно висвітлює діяльність Комуністичної партії Китаю чи уряду, то погіршиться рейтинг не тільки автора, а і його оточення.

В 2016 році Державна рада Китаю оновила документ під назвою “Механізми попередження та покарання людей, схильних до порушень” [22], яким було передбачено санкції для власників низьких рейтингів: заборона на роботу в держустановах; відмова в соцзабезпеченні; особливо ретельний огляд на митниці; заборона на зайняття керівних посад в харчовій і фармацевтичній промисловості; відмова в авіаквитках і спальному місці в нічних поїздах; відмова в місцях в люксових готелях і ресторанах; заборона на навчання дітей в дорогих приватних школах.

Система передбачає також рейтинги юридичних осіб на основі відповідності їх діяльності екологічним, юридичним нормам, умов і безпеки праці, фінансової звітності. Якщо ніяких претензій немає – компанії присвоюється високий рейтинг і користується пільговим режимом оподаткування, хорошими умовами кредитування, спрощеними адміністративними процедурами тощо. Підприємства з низьким рейтингом, відповідно, мають дорогі кредити, підвищені ставки податків, заборону на емісію цінних паперів, заборону на інвестування в компанії, акції яких продаються на біржі, а також

необхідність отримувати державний дозвіл на інвестування навіть в ті галузі, доступ до яких в принципі не є обмеженим.

Не залишились поза увагою при формуванні системи соціального кредиту і владні діячі. Наприклад, партійна школа при Комітеті Комуністичної партії Китаю провінції Сичуань підписала з Університетом електроніки і технологій КНР угоду про створення першої в країні системи рейтингів і оцінки надійності для чиновників низового рівня. Система під назвою “Розумна червона хмара” за допомогою технологій штучного інтелекту і Великих Даних буде аналізувати дані про кожного чиновника, наприклад, відвідуваність партійних зборів, освіту, сімейний стан, зіставляти дані про доходи чиновника і членів його сім’ї з даними щодо придбаної нерухомості і предметів розкоші, а на підставі цих даних, а також інформації про активність чиновника в соцмережах буде оцінюватися ступінь його політичної благонадійності. Відзначається, що таким чином можна буде набагато ефективніше передбачати поведінку чиновника, оцінювати його моральне обличчя і виявляти потенційних корупціонерів [22].

“Цифрова диктатура” – термін, яким з “легкої руки” американських журналістів прозвали проект системи соціального кредитування Китаю, має певні логічні аргументи для вжитку. Пригадаємо шість базових характеристик тоталітаризму, сформульованих К. Фрідріхом у роботі “Природа тоталітаризму” (1954 р.): офіційна ідеологія, яка претендує на охоплення всіх аспектів людського існування і орієнтується на досягнення одвічних цілей, наприклад, на створення досконалого суспільства; масова партія, яка зливається з державною бюрократичною організацією; монополія партії над ефективними засобами комунікації; концентрація в руках партії і держави всіх засобів збройного насильства; централізований контроль і керівництво економікою; система терористичної поліцейської влади [23, с. 278].

Фактично, в Китаї відбулося встановлення диктатури комуністичної партії, яке призвело до злиття партійних структур з державними і до формування своєрідного феномена “держава-партія”. Партія монополізувала право виступати від громадянського суспільства в державі. Влада поширює контроль на всі сторони життя людини, включаючи сімейні відносини і сферу відпочинку. Як відзначила Х. Арендт, при тоталітаризмі був реалізований принцип: “приватною особою залишається тільки той, хто спить” [23, с. 279].

Досліджуючи ці процеси мимоволі повстає в пам’яті антиутопія англійського письменника Джорджа Орвелла “1984”. Однак, це не літературний шедевр, а дійсність найбільшої за чисельністю населення країни (понад 1,38 млрд осіб), яка є одним з основних геополітичних акторів, лідером електронної комерції, і чиї інвестиції у світову економіку постійно зростають, в тому числі – в Україні. У 2016 році Китай інвестував за кордон приблизно $ 170 млрд, при цьому китайці купили 309 європейських підприємств на суму $ 85,8 млрд. Китай продовжує свою експансію на закордонні ринки в ролі стратегічного інвестора. Згідно з новою стратегією, протягом найближчих 5 років КНР має намір інвестувати $ 120 – 130 млрд в економіку зарубіжних країн. Згідно з даними китайського посольства, китайські інвестиції в Україну за весь період взаємин країн склали близько $ 7 млрд [24].

Уряд Китаю хоче реалізувати довгостроковий план, використовуючи багатство і промислові ноу-хау Китаю, щоб очолити глобалізацію 2.0, яка ігноруватиме правила західних інституцій. Мета полягає у тому, щоб перекроїти глобальний економічний порядок, притягуючи країни та компанії на китайську орбіту. Про це пише “The New

York Times”, посилаючись на директора Центру міжнародного співробітництва Національної комісії розвитку і реформ Као Венліан [26].

Таким чином, будуючи мости, аеропорти, залізниці і електростанції Китай закріплює за собою можливості впливу через інфраструктуру. Не оминули ці проекти і Україну, наприклад, китайці допомагають модернізувати Укртелеком, незважаючи на низку негативних новин про невиплату компанією і її акціонером мільярдних боргів по облігаціях. China Development Bank і Huawei, які стали головними інвесторами, в разі непогашення боргу в рахунок застави за мільярди кредитів можуть отримати деякі будівлі компанії, обладнання, що буде надано компанією Huawei, а також Укртелеком надав китайському банку права вимоги за деякими банківськими рахункам [26]. Таким чином, майно однієї з основних компаній ринку телекомунікаційних послуг України, яка забезпечує діяльність інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, ймовірно може опинитися у власності китайських компаній, які контрольовані владою цієї країни.

Висновки.

Порівнюючи цінності, що ставляться на чолі електронної демократії, і порушення прав людини, які тягне за собою цифрова диктатура, визначимо наступне:

1. Інформаційне суспільство, як стадія технологічного розвитку людства, не визначає змістовного наповнення соціальних процесів, а лише виступає формою реалізації існуючої форми правління в державі, що відображає політичну організацію суспільства в ній.

2. Інтеграція інформаційних технологій в усі сфери життя людини і суспільства інтенсифікує політико-правові процеси в державі і суспільстві незалежно від форми політичного режиму. В демократичному суспільстві впровадження ІКТ покликане інтенсифікувати демократичні процеси, надати членам суспільства ширші можливості і більш ефективні інструменти участі у здійсненні влади. Хоча не слід ідеалізувати ці процеси, оскільки існують ризики, наприклад, незаконного використання персональних даних громадян приватними корпораціями. Але демократична держава за таких умов має правові та економічні важелі впливу на правопорушника.

Тоді як в недемократичному режимі інформаційні технології використовуються для вдосконалення систем тотального контролю за громадянами з боку держави, створення контрольованого суспільства і така влада не може бути обмежена в жоден спосіб.

3. І третій, але не останній висновок, стосується не стільки теорії держави і права, скільки політико-правової картини світу. Політичний режим не може бути приватною справою кожної держави. Адже інформатизація суспільства прискорює його глобалізацію. І зіткнення різних культур, релігій, ідеологій, політичних режимів стає неминучим.

За словами лорда Уінстона Леонарда Спенсера Черчіля, “Демократія – найгірша форма правління, та людство нічого кращого поки не придумало”. Тож, доки нічого кращого не буде винайдено, людству необхідно змагатись за демократичні цінності – виборність влади, верховенство закону, незалежну судову владу, дієве громадянське суспільство, дотримання основоположних прав і свобод людини. Інакше наступним цивілізаційним етапом людства стане рабовласницький лад. Цифрове, електронне чи кіберрабство – ймовірно, наукова дискусія щодо понятійного апарату буде вже недоречною.

Використана література

1. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/537-16

2. Окінавська хартія глобального інформаційного суспільства. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/998_163

3. Масуда Й. Комп’ютопія ; [пер. з англ. В. Ляха] / Філософська і соціологічна думка. – 1993. – № 6. – С. 36-50.

4. Бєляков К., Ланде Д., Ніконова В. Інформаційне законодавство : новели 2013 року // Юридчний Вісник України. – № 52 (965). – С. 14-15. – (28.12.13 р. – 3.01.14 р.).

5. Digital Democracy. The tools transforming political engagement / Simon J., Bass T., Boelman V., Mulgan D. – London, Nesta, 2017. – 100 p.

6. Cyberdemocracy: Technology, Cities and Civic Networks / Tsagarousianou R.,Tambini D., Bryan C. – NY, Routledge New York, 1998. – 200 p.

7. Poster M. CyberDemocracy: Internet and the Public Sphere. – Irvine, University of California, 1995. – Режим доступу : http://www.faculty.humanities.uci.edu/poster/writings/democ.html

8. Брижко В. е-майбутнє та інформаційне право / [В. Брижко, Ю. Базанов, М. Швець та ін.] ; за ред. доктора економічних наук, професора, члена-кореспондента Академії правових наук України М. Швеця. – [2-е вид., доп.]. – К. : НДЦПІ АПрН України. – 2006. – 233 с.

9. Грицяк Н.В. Електронна демократія : навч. посіб. / Н.В. Грицяк, С.Г. Соловйов ; за заг. ред. д-ра наук з держ. упр., проф. Н.В. Грицяк. – К. : НАДУ, 2015. – 66 с.

10. Концепція розвитку електронного урядування в Україні : Розпорядження Кабінету Міністрів України від 13.12.10 р. № 2250. // Офіційний вісник України, 2010 р. – № 97. – Ст. 3443.

11. Стратегія державної політики сприяння розвитку громадянського суспільства в Україні : Указ Президента України № 212 від 24.03.12 р. – Режим доступу : http://www.president.gov.ua/documents/682016-19805

12. План дій з впровадження в Україні ініціативи “Партнерство “Відкритий Уряд” : Розпорядження Кабінету Міністрів України від 05.04.12 р. № 220. – Режим доступу : http://zakon3. rada.gov.ua/laws/show/909-2016-%D1%80

13. Концепція розвитку електронної демократії та план заходів з її реалізації : Розпорядження Кабінету Міністрів України від 07.11.17 р. – Режим доступу : http://www.dknii.gov.ua/content/uryad-shvalyv-koncepciyu-rozvytku-elektronnoyi-demokratiyi

14. Recommendation Rec(2004)15 of the Committee of Ministers to member states on electronic governance. – Режим доступу : https://wcd.coe.int/ViewDoc.jsp?p=&Ref=Rec(2004)15&Language=lanEnglish&Ver=original&direct=true

15. Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy. – Режим доступу : https://www.coe.int/t/dgap/democracy/activities/ggis/cahde/2009/RecCM2009_1_and_Accomp_Docs/Recommendation%20CM_Rec_2009_1E_FINAL_PDF.pdf

16. Що ж таке електронна демократія? – (Блог Олександра Гирича). – Режим доступу : http://dialog.lviv.ua/shho-zh-take-elektronna-demokratiya

17. Проект плану зі створення системи соціального кредиту довіри (КНР, 2014 – 2020 рр). – Режим доступу : https://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

18. Деякі зауваження канцелярії Держсекретаря КНР про створення системи соціального кредитування. – Режим доступу : https://www.gov.cn/zhengce/content/2016-06/12/content_5081222.htm

19. China’s plan to organize its society relies on ‘big data’ to rate everyone . – Режим доступу : https://www.washingtonpost.com/world/asia_pacific/chinas-plan-to-organize-its-whole-society-around-big-data-a-rating-for-everyone/2016/10/20/1cd0dd9c-9516-11e6-ae9d-0030ac1899cd_story.html?utm_term=.1d087434bf35

20. China’s New Tool for Social Control: A Credit Rating for Everything . – Режим доступу : https://www.wsj.com/articles/chinas-new-tool-for-social-control-a-credit-rating-for-everything-1480351590

21. Цифровая диктатура : как в Китае вводят систему социального рейтинга . – Режим доступу : http://www.rbc.ru/business/11/12/2016/584953bb9a79477c8a7c08a7

22. Використання Великих Даних + штучний інтелект “для розрахунку ідеологічного статусу членів партії”. – Режим доступу : http://digitalpaper.stdaily.com/http_www.kjrb. com/ kjrb/html/2017-06/30/content_372603.htm?div=-1

23. Цитата за Юрій М.Ф. Політологія : підручник. – К., Дакор, 2006. – 416 с

24. Китайские инвестиции в Украине / Инвестиционная аналітика. – (01.07.17 г.). – Режим доступу : https://inventure.com.ua/analytics/investments/kitajskie-investicii-v-ukraine-schitaem-na-palcah

25. Behind China’s $1 Trillion Plan to Shake Up the Economic Order // The New York Times, May 13, 2017 . – Режим доступу : https://www.nytimes.com/2017/05/13/business/china-railway-one-belt-one-road-1-trillion-plan.html?_r=1

26. Укртелеком под залог, или почему китайцы не боятся рискнуть / “Ліга-Бізнес”, 04.06.2017 г.. – Режим доступу : http://biz.liga.net/all/telekom/stati/3687202-ukrtelekom-pod-zalog-ili-pochemu-kitaytsy-ne-boyatsya-risknut.htm

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

Правова інформатика

УДК 002.6:004:340.1+316.329.8

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

ІНТЕРНЕТ РЕЧЕЙ (IoT): ПРАВОВІ ПРОБЛЕМИ ЗАСТОСУВАННЯ РОЗУМНИХ КОНТРАКТІВ

Анотація. *Аналізується застосування так званих розумних контрактів, які отримали поширення в останні роки. Надається визначення терміну “розумний контракт”, пропонується певна їх класифікація. Проведено порівняльний аналіз традиційних та розумних контрактів в частині особливостей правового регулювання їх застосування. Сформульовані правові проблеми теоретичного та практичного спрямування, які є суттєвим бар’єром на шляху застосування розумних контрактів в умовах широкого використання технологій Інтернету речей, для деяких з них запропоновано шляхи вирішення.*

Ключові слова*: розумний контракт, Інтернет речей, алгоритм, програмування, захист.*

Summary. *The analysis of using so-called smart contracts, which have become widespread in recent years. The definition of the term “smart contract” is given, some classification is offered for them. A comparative analysis of traditional and smart contracts in the part of legal regulation of their application was conducted. The article formulates legal problems of the theoretical and practical direction, which are a significant barrier to the use of smart contracts in the context of widespread use of Internet of Things, some solutions have been suggested for them.*

Keywords*: smart contract, Internet of Things, algorithm, programming, protection.*

Аннотация*. Анализируется применение так называемых умных контрактов, получивших распространение в последние годы. Предлагается определение термина “умный контракт” и определенная их классификация. Проведен сравнительный анализ традиционных и умных контрактов в части особенностей правового регулирования их применения. Сформулированы правовые проблемы теоретического и практического направления, которые являются существенным барьером на пути применения умных контрактов в условиях широкого использования технологий Интернета вещей, для некоторых из них предложены пути решения.*

Ключевые слова*: умный контракт, Интернет вещей, алгоритм, программирование, защита.*

Постановка проблеми. Світ знаходиться на порозі початку тотального використання технологій Інтернету речей, орієнтованих на дистанційне надання послуг і проведення робіт в найрізноманітніших сферах людської діяльності за участю або без участі людей, але в інтересах фізичних і юридичних осіб. У цих умовах особливого значення набуває можливість за участю або без участі людини дистанційно укладати і виконувати договори на основі використання інформаційно-комунікаційних технологій, які отримали назву розумні контракти. Тому останнім часом увагу багатьох вчених і практиків привертає проблематика розумних контрактів.

Ще в 1997 році М. Сабо констатував, що наслідки розробки розумних контрактів відповідно до договірного права, а також розробки стратегічних контрактів на середину 1990-х років мало вивчені, незважаючи на величезні перспективи, особливо у разі використання елементів штучного інтелекту, які також мало вивчені [10].

В даний час розумні контракти досить широко, як для нового явища, увійшли в практику договірних відносин. Найбільш яскравим прикладом може служити біткойн, як всесвітня пірінгова криптовалютна цифрова платіжна система, яка використовує однойменну розрахункову одиницю і однойменний протокол передачі даних [3]. Але, тим не менш, не уявляється можливим констатувати якісь значні успіхи юридичної науки в дослідженні проблематики розумних контрактів за минулі 20 років.

У дискусії про розумні контракти можна умовно виокремити два основних підходи:

розумні контракти – це коли суспільні відносини регулюються програмним забезпеченням (комп’ютерним кодом) [12];

розумні контракти – це коли при реалізації суспільних відносин використовується програмне забезпечення, що відповідає певним домовленостям або положенням закону.

Відносно першого підходу викладемо такі міркування. Відомо, що люди (програмісти) створюючи програмне забезпечення, керуються певними алгоритмами реалізації якихось дій (обчислень, обробки даних, функціонування технічних виробів, поведінки людей тощо). Ці алгоритми створюються людьми, які відображають в них своє розуміння порядку або правил реалізації певних дій, але розуміння, яке детермінується відомими закономірностями математики, фізики, механіки, металообробки, електроніки, робототехніки тощо, а в разі людей – соціальними регуляторами, в тому числі – правовими нормами.

Таким чином, поки програмні засоби для розумних контрактів створюються людьми або під керівництвом людей можна сміливо стверджувати, що перший підхід, який базується на твердженні – “суспільні відносини регулюються програмним забезпеченням”, принципово спотворює сприйняття ролі та місця комп’ютерних кодів в суспільних відносинах.

Однак слід зауважити, що незважаючи на таку фундаментальну методологічну помилку деяких авторів – прихильників цього метафізичного підходу, не можна безапеляційно повністю відкидати отримані ними наукові результати, частина з яких може бути досить продуктивною для розвитку юридичної теорії та практики розумних контрактів.

Виходячи з вище викладеного, в цій роботі буде приділено увагу розвитку другого підходу. На наш погляд, дослідження теоретико-методологічних і законодавчих проблем правового регулювання застосування інноваційних розумних контрактів, особливо в умовах широкого використання технологій Інтернету речей з метою створення сприятливих умов для їх широкого застосування в людській і юридичній практиці, є актуальним завданням.

Мета статті полягає у визначенні проблем правового регулювання застосування розумних контрактів в умовах функціонування технологій Інтернету речей.

Виклад основного матеріалу. Історично першим було визначення сформульоване Н. Сабо: “розумний контракт – це набір обіцянок, зазначених в цифровій формі, включаючи протоколи, в якій сторони виконують ці обіцянки” [10].

Але в сучасній юридичній літературі як немає досі єдиного визначення Інтернету речей, так немає і єдиного визначення терміну “розумний контракт”.

У своїй досить системній статті А.І. Савельєв дає наступне визначення: розумний контракт – це договір, який існує в формі програмного коду, що імплементовано на платформі Blockchain, який забезпечує автономність і самовиконання умов такого договору у разі настання заздалегідь визначених в ньому обставин [21].

Головна мета створення розумного контракту – автоматизація взаємовідносин різних сторін, побудована на основі алгоритму, якому кожна зі сторін надала право від

свого імені здійснювати певні дії відповідно до низки вимогливо заданих умов. Іншими словами, розумний контракт – це одночасно і набір правил, і робот, який від імені свого “господаря” вчиняє дії за заданими правилами, в тому числі такі, що впливають на правовідносини [18].

Старк Д. вважає, що термін “розумний контракт” відноситься до випадку використання комп’ютерного коду у вигляді мови програмування, наприклад javascript або HTML, для формулювання, перевірки і виконання угоди між сторонами, що фактично стає еквівалентною заміною контракту, написаного природною людською мовою [5]. При цьому розумний контракт “виконується” комп’ютером з урахуванням умов угоди.

В роботі, присвяченій транскордонним аспектам, Хурані С. вважає, що розумні контракти – це програмні коди, в які вбудовуються умови контракту і які працюють в мережі, що призводить до часткового або повного автоматизованого самовиконання контракту [13].

Смарт-контракти за М. Раскіним – це угоди, що виконуються автоматизовано за допомогою комп’ютерних програм, що мають контроль над фізичними або цифровими об’єктами, реалізація яких відбувається без людського впливу і звернення до суду [9].

Отже, аналізуючи наведені та багато інших дефініції визначення “розумний контракт”, можемо виділити те спільне, що їх об’єднує: це набір обіцянок, зазначених в цифровій формі; це набір правил; це договір, який існує в формі програмного коду, що імплементовано на платформі блокчейн [*]; це договір, який самостійно виконується у разі настання заздалегідь визначених в ньому обставин; це набір комп’ютерного коду, який використовується для формулювання, перевірки і виконання договору; це програмні коди, в які вбудовуються умови контракту і які працюють в мережі і є еквівалентною заміною контракту, що “виконується” комп’ютером; це угоди, що виконуються автоматизовано за допомогою комп’ютерних програм, реалізація яких відбувається без людського впливу.

Слід зауважити, що всі дефініції визначення “розумний контракт” безпосередньо або опосередковано в наступних поясненнях містять посилання на використання технології або платформи блокчейн. Це можна пояснити тим, що саме з розробкою технології блокчейн-ланцюжків створилася можливість більш-менш ефективно втілити в життя ідею розумних контрактів, завдяки особливим властивостям цієї технології.

Однак, зовсім недавно було повідомлено про те, що з’явився конкурент технології блокчейн. Голова ради директорів і головний технологічний директор Oracle Ларрі Еллісон розповів про нову розробку – першої в світі 100 % самокерованої автономної бази даних – Oracle Autonomous Database Cloud на основі Oracle Database 18c, яка використовує алгоритми машинного навчання і практично не вимагає адміністрування та налаштування, усуваючи ймовірність помилки через “людський фактор” і функціонуючи подібно до самокерованих автомобілів [22]. Крім того, як підкреслив Ларрі Еллісон, вирішується досить актуальна сьогодні проблема кібербезпеки: бази даних можуть самі себе захищати, виявляючи аномальні події, наприклад, якщо хтось раптом увійде в систему з нетипового регіону. Повністю автоматизована СУБД здатна також виявляти і припиняти атаки, автоматично застосовувати патчі в реальному часі: зупиняти базу даних для цього не потрібно.

[*] *Від ред.* Блокчейн – це технологія, яка визначає ланцюг інформаційних блоків, які здійснюють обробку даних на різних комп’ютерах.

Тому з метою формулювання дефініції терміну “розумний контракт” в юридичній конотації вважаємо недоцільним згадку в ній назви конкретної технології виходячи з принципу технологічної нейтральності правового регулювання. Технології можуть детермінувати особливості правового регулювання, але не визначати його сутність. Інакше з появою кожної нової технології довелося б переписувати закони. А як бути, коли в соціальних відносинах буде одночасно використовуватися набір різних технологій? Тому в подальших дослідженнях будемо розглядати приклади з використанням блокчейн-ланцюжків тільки з метою визначення особливостей правового регулювання при їх використанні в договірних відносинах.

Сформулюємо в інтересах юридичних досліджень таку дефініцію: розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається за участю або без участі людини, але з використанням мережевих комп’ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв’язок з фізичними або цифровими об’єктами.

Відмінною рисою цього визначення є те, що розумний контракт визнається еквівалентом традиційного контракту, який за допомогою ІКТ може укладатися, виконуватися і припинятися за участю або без участі людини. Участь людини може проявлятися навіть в простому ініціюванні виконання розумного контракту. Крім того, це визначення інваріантне до типу використовуваних технологій і до типу використовуваних мов програмування.

Зазвичай, в літературі вказують на такі переваги застосування розумних контрактів, заснованих на використанні блокчейнів [11; 14; 15]:

1. Висока швидкість – використання смарт-контрактів, дозволяє значно прискорити бізнес-процеси.
2. Ефективність – для повторюваних, однотипних контрактів.
3. Достовірність – принцип побудови блокчейн-ланцюжків виключає внесення змін до його тексту змін, не санкціонованих усіма сторонами контракту.
4. Спостережність – прозорість і простота звітності про вчинені транзакції.
5. Економічність – зменшення транзакційних витрат завдяки виключенню посередників, зменшення витрат людської праці.
6. Надійність – мінімізація ризику виникнення механічної помилки в процесі виконання контракту, можливість відновлення даних у разі їх втрати, висока стійкість проти кіберзагроз.
7. Універсальність – можливість застосування в найрізноманітніших сегментах людської діяльності.

Справедливості заради, слід зазначити, що не всі поділяють ентузіазм з приводу розумних контрактів.

Деякі дослідники вважають, що на даному етапі “розумний” контракт здебільшого являє собою кращий спосіб автоматизованого виконання досягнутих домовленостей, такий своєрідний спосіб їх виконання, ніж традиційний контракт (договір), що представляє собою сформульований набір домовленостей сторін, які досягнуті за допомогою переговорного процесу. Таким чином, вони припускають, що можливий сценарій, відповідно до якого сторони укладають звичайний договір та передбачають в ньому механізми виконання із застосуванням автоматизованих алгоритмів (“розумних” контрактів). Разом з тим, вони стверджують, що звичайний “паперовий” договір повинен в будь-якому випадку мати пріоритет над “розумним” контрактом [17].

Смарт-контракти можуть також спричинити нові проблеми, вважають в юридичній фірмі Strafford Kent Law (Nottingham, England), а деякі варіанти їх використання просто

неможливі. В результаті юридичного аналізу вони доходять такого висновку: в реальному житті складно розглядати інтелектуальний контракт як розумний, так і як контракт тому, що в даний час це просто автоматизований комп’ютерний код. Отже, застосування терміну “розумний контракт” певним чином вводить в оману, тому, можливо, краще відмовитися від нього. Більш відповідною назвою, ймовірно, буде інтелектуальний агент або інтелектуальна програма [15].

Напевно, важко повною мірою опротестувати такі висновки, оскільки ряд практичних кейсів, які сьогодні називають розумними контрактами, такими дійсно не є, але, в той же час, з’являється дедалі більше прикладів дійсно розумних контрактів, які повністю виконуються за допомогою мережевих комп’ютерних програмних та/або програмно-апаратних засобів. Тому реальні чи уявні перспективи застосування стимулюють проведення правових наукових досліджень в сфері застосування розумних контрактів.

Зазвичай наукові дослідження починаються з вивчення питань класифікації, що дозволяє згодом провести певну декомпозицію об’єкта дослідження і спростити його вивчення. У проблематиці розумних контрактів було запропоновано класифікувати їх на сильні і слабкі [9]. На думку М. Раскіна під сильними розумними контрактами слід розуміти ті, для яких їх анулювання та модифікація призводять до надмірно високих витрат, а слабкі розумні контракти – це ті, які таких витрат не мають. Далі несподівано з’являється парадоксальний висновок про те, що суду не має сенсу своїм рішенням змінювати сильний контракт після його виконання, оскільки це призведе до непомірно високих витрат.

У багатьох юрисдикціях сторонам договору надається конституційне право на звернення до суду для захисту своїх інтересів або порушених прав. Тому запропонований підхід призводить до ситуації оцінки розумних контрактів тільки як слабких, тобто таких, в яких всі дії сторін строго детерміновані та не допускають неоднозначного розвитку подій, що вимагає певного вибору для кожної зі сторін, а це, на нашу думку, різко звужує можливі сфери застосування розумних контрактів.

Тому запропонуємо класифікувати розумні контракти на саморегульовані і на регульовані відповідно до загального договірного права.

З огляду на поширений в національних юрисдикціях принцип свободи договору є цілком логічним припущення, що певна спільнота суб’єктів може встановити всередині себе деяку сукупність правил здійснення розумних контрактів, що прямо не передбачені законодавством, але і не суперечать договірному праву, які дозволяють мінімізувати контрактні помилки, що призводять до виникнення спірних ситуацій.

Спільноту, в якій регулювання всіх суспільних відносин здійснюється на основі нею створених правил, будемо називати саморегульованою, а розумні контракти, які будуть використовуватися для формалізації взаємовідносин між членами цієї спільноти, будемо називати саморегульованими розумними контрактами.

Крім того, співтовариство в рамках своїх правил також може встановити порядок розгляду можливих спорів без звернення до суду. Такий підхід дозволяє істотно скоротити витрати, пов’язані з судовим розглядом суперечок, в будь-якій предметній сфері застосування розумних контрактів.

Таким чином, м’яке право, виражене в правилах саморегульованої спільноти матиме високу ефективність, якщо оголошені правила в частині укладення, виконання та припинення розумних контрактів не містять внутрішніх протиріч, які можуть стати причиною виникнення суперечок, і приймаються беззастережно всіма членами

спільноти. Як показує практика, такий підхід досить успішно реалізується в закритих пірінгових платіжних системах.

У той же час, правила саморегульованої спільноти повинні бути такими, щоб забезпечувати юридично дозволену поведінку її членів з метою мінімізації втручання державних інституцій, наприклад, в разі правопорушень. З юридичної точки зору система правового регулювання взаємовідносин саморегульованої спільноти з кандидатами в її члени може мати в якості аналогії публічний договір.

Однак при цьому доцільно розробити вичерпні, прозорі і не надмірні правові механізми для проведення, в разі необхідності, інспектування правоохоронними органами на відповідність закону предметів розумних контрактів, які виконуються в межах саморегульованих спільнот, з мінімізацією або виключенням порушення виконання цих контрактів та з встановленням юридичної відповідальності для посадових осіб за зловживання владою.

Цілком очевидно, що необхідно провести дослідження для виявлення особливостей системи правового регулювання в різних галузях застосування розумних контрактів за умови використання мережевих комп’ютерних технологій з метою максимального зменшення транзакційних витрат і зниження бар’єрів при розгляді спорів в суді. Перш за все, звичайно, необхідно визначитися з юридичним статусом розумного контракту як контракту, який укладається, виконується і припиняється з використанням мережевих комп’ютерних програмних та/або програмно-апаратних засобів.

У деяких роботах пропонується визнавати юридичний статус розумних контрактів відповідно до положень Конвенції ООН про використання електронних повідомлень у міжнародних договорах на підставі наступного [13]:

розумний контракт формується в електронному вигляді за допомогою комп’ютерного коду (стаття 1);

розумні контракти, сформовані в результаті автоматичних повідомлень, є юридично дійсними та підлягають виконанню відповідно до Конвенції (стаття 12).

В результаті критичного аналізу можна констатувати, що:

Конвенція застосовується лише в разі використання електронних повідомлень в зв’язку з укладанням чи виконанням договорів між сторонами, але таких, які викладені природньою мовою, яку безпосередньо сприймає людина (стаття 1). Тому вона не може бути застосована у випадку повідомлень, представлених виключно у вигляді програмного коду;

положення Конвенції поширюються на використання автоматизованих систем повідомлень, але повідомлень, які викладені природньою мовою, оскільки в Конвенції згадується “про взаємодію автоматизованої системи повідомлень і будь-якої фізичної особи...”. Тому положення Конвенції не можуть застосовуватися до випадків з повідомленнями, представленими виключно у вигляді програмного коду.

Таким чином, уявляється помилковою пропозиція щодо визнання юридичної сили розумного контракту на підставі положень Конвенції ООН про використання електронних повідомлень в міжнародних договорах.

Цивільний кодекс України встановлює, що в письмовій формі повинні укладатися всі контракти між юридичними особами, юридичними і фізичними особами (за винятком усних), між фізичними особами, якщо сума договору двадцятикратно перевищує розмір неоподатковуваного мінімуму (на сьогодні – це 17 грн.).

У статті 207 ЦКУ законодавець встановив умови того, коли контракти, вчинені з використанням електронних документів, можуть вважатися укладеними в письмовій формі. Ці вимоги, звичайно, відносяться до документів (інформаційних повідомлень)

викладених природньою мовою. При цьому допускається використання спеціального електронно-цифрового підпису, який відповідно до закону є еквівалентом власноручного підпису.

Виходячи з цього, виникає проблема необхідності розробки правових механізмів для розумних контрактів в частині:

визнання “тексту” договору, викладеного в комп’ютерному коді, еквівалентним письмовій формі;

визнання систем верифікації сторони контракту, які використовуються в мережевих комп’ютерних програмних та/або програмно-апаратних засобах, еквівалентними законодавчо схваленим системам ідентифікації суб’єктів за допомогою електронного або електронно-цифрового підпису;

визначення місця укладення контракту з урахуванням можливої різної національної юрисдикції і мобільності сторін договору, наприклад, якщо сторона договору перебуває на борту літака, що летить;

нотаріального посвідчення та державної реєстрації розумних контрактів.

Таким чином, для розумних контрактів, які повністю ускладаються та/або виконуються за допомогою мережевих комп’ютерних програмних та/або програмно-апаратних засобів, реалізованих з використанням певної мови програмування, необхідно провести ретельний аналіз системи правового регулювання в частині забезпечення формальних вимог до укладання контрактів. Це стосується, перш за все, вимоги щодо письмової форми укладання контракту, нотаріального засвідчення та державної реєстрації контракту, визначення місця укладення контракту тощо.

Різні етапи договірних відносин (укладення, виконання та припинення) мають різний ступінь ризику виникнення суперечок.

На першому етапі договірних відносин в переважній більшості випадків ймовірність виникнення спору дуже низька, оскільки сторони добровільно погоджуються на виконання умов, обговорених в контракті, в тому числі й в розумному.

У національних юрисдикціях, як правило, закріплено принцип презумпції правомірності укладених контрактів, як, наприклад, в статті 204 Цивільного кодексу України. Винятки становлять лише пряма вказівка в законі на недійсність договору або якщо недійсним його визнає суд. Крім того, в законодавстві формулюють загальні вимоги, виконання яких є обов’язковим для того, щоб контракт вважався дійсним, наприклад, відсутність суперечності законодавству, наявність цивільної дієздатності, вільне волевиявлення, дотримання встановленої форми укладення, націленість на досягнення реальних правових наслідків тощо.

Однак найбільша кількість суперечок може виникати на етапі виконання. Це пов’язано, як це часто буває в реальній практиці виконання контрактів, з необхідністю узгодженої зміни певних умов його виконання або зміни загальних умов його виконання, що потребує створення юридичних і технологічних можливостей для внесення змін в розумні контракти шляхом зміни програмного забезпечення. Оскільки доктрина загального права щодо реального виконання дозволяє визнати контракт навіть в тому випадку, якщо його виконання не в повному обсязі відповідає викладеним в ньому певним умовам [9], то внесення таких змін може бути не обов’язковим, що надає можливість сторонам провести дослідження в кожному конкретному випадку для відносної оцінки необхідних витрат на модернізацію розумного контракту й шкоди для сторін в разі відсутності зміни програмного забезпечення.

Як вже раніше зазначалося, у всіх відомих на сьогодні прикладах застосування розумних контрактів укладення, виконання та припинення відбувається з

використанням мережевих комп’ютерних програмних та/або програмно-апаратних засобів, які реалізовані на технології (платформі) блокчейн-ланцюжків. Застосування блокчейн-платформ для реалізації розумних контрактів призводить до необхідності дослідження особливостей правового регулювання використання розумних контрактів.

Одним з ключових питань для урядів є питання про те, чи повинні законодавчі положення регулювати всі потенційні застосування технології блокчейн або повинні обмежуватися лише певними галузями і випадками їх застосування. Банківська і фінансова індустрія є наочним прикладом галузі, яка, ймовірно, вдасться до жорстких заходів контролю щодо технологій, заснованих на технології “блокчейн” [8].

Серед експертів існують різні точки зору на оцінку можливого використання розумних контрактів.

Деякі з них вважають, що найбільші перспективи має модель, коли розумні контракти реалізуються в рамках традиційної правової системи, визнаючи при цьому, що розумні контракти не повинні замінювати ні традиційне договірне право, ні традиційних юристів за контрактом [11]. Крім того, вони вважають, що традиційне договірне право, зокрема вимоги до правил доведення, можливо, необхідно буде змінити, з урахуванням автоматизованого і детермінованого характеру розумних контрактів, а також питань, пов’язаних з можливістю їх реалізації.

Поява розумних контрактів, швидше за все, може призвести до переоцінки загальноприйнятої практики договірного права в міру того, як юристи будуть визначати, які типи угод і термінів найкраще підходять для програмування та автоматичного виконання, а які слід залишити для складання природною мовою [5].

Тому проаналізуємо можливі відмінності або схожість в процесі складання розумного контракту і традиційного контракту як угод про реалізацію суспільних відносин в якійсь предметній сфері.

При укладанні, виконанні та припиненні будь-якого контракту, який визнається національною або міжнародною правовою системою, сторони мають на меті зробити і роблять певні дії, детерміновані правовими нормами контракту або законодавства, відповідно до певного алгоритму, зміст якого великою мірою визначається власне конкретним типом контракту. Або, іншими словами, будь-який контракт є описом алгоритму дій його сторін при взаємодії одна з одною для досягнення мети контракту. В даному випадку алгоритм означає певну послідовність дій сторін контракту, що здійснюються в рамках традиційної системи права відповідно до класичної структури правової норми: гіпотеза, диспозиція і санкція. У класичній лексиці алгоритмів структура правової норми виглядає так:

– ***якщо*** – опис гіпотези як опису деякої сукупності зовнішніх і внутрішніх умов або опису стану сторін, які є виключною підставою для початку виконання окремих елементів контракту;

– ***то*** – опис диспозиції як опису сукупності певного набору дій сторонами контракту, які обов’язково виконуються при настанні умов, описаних гіпотезою;

– ***інакше*** – опис санкцій як опису деякої сукупності дій по відношенню до сторони контракту, що не виконала вимог диспозиції, які дозволяють компенсувати збитки, завдані іншій стороні невиконанням положень контракту.

Ухвалення формального алгоритмічного підходу, обґрунтованого самою структурою правових норм, при складанні комп’ютерної програми, що реалізує укладання, виконання і припинення розумного контракту відкриває шляхи до найрізноманітніших способів перетворення природної юридичної мови (мови складання традиційного контракту) в мову (лексику) програм, “зрозумілих” обчислювальним

машинам. Оскільки розумні контракти передбачають використання ІКТ, то ця обставина уявляється досить важливою.

Таким чином, можемо висунути гіпотезу про те, що існує принципова можливість еквівалентного перетворення алгоритму дій, який закладається в традиційний контракт за допомогою викладання правових норм природньою юридичною мовою, у відповідний комп’ютерний алгоритм, що створює сприятливі умови для подальшого створення контрактів у вигляді комп’ютерних програм (комп’ютерних кодів).

Для визначення вимог до апаратно-програмного забезпечення розумних контрактів Н. Сабо виділяє чотири необхідних функціональних властивості звичайних контрактів [10]:

1. Спостережність – здатність сторін спостерігати за виконанням контракту іншою стороною або доводити свою ефективність третім особам.

2. Верифікованість – здатність сторін контракту довести арбітру, що контракт був виконаний або порушений, або здатність арбітра визначити це іншими способами.

Спостережність та верифікованість створюють умови для своєчасної індикації навмисних порушень контракту або помилки сумлінності.

3. Секретність (privity) – принцип, згідно з яким знання та контроль за змістом і виконанням контракту повинні розподілятися між сторонами лише в тому обсязі, наскільки це необхідно для виконання цього контракту.

4. Здатність до виконання – реалістичність виконання контракту, що мінімізує необхідність в забезпеченні дотримання виконання контракту.

Деякі дослідники вважають, що оскільки транзакції розумного контракту запрограмовані в блокчейне, то закодований характер дозволяє сторонам висловлювати умови контракту менш складними способами, ніж якби умови були написані простою мовою на папері [1].

Інші ж автори вважають, що сфера застосування розумних контрактів обмежена, оскільки контракти природньою мовою завдяки багатій семантиці дозволяють моделювати життєві ситуації з досить великим ступенем абстракції [17; 18].

Але велика ступінь абстракції – це скоріше недолік, а не перевага контрактів укладених природньою мовою, оскільки вона обумовлює великий ступінь невизначеності при виконанні контрактів, що неминуче може призводити і призводить до виникнення суперечок. На проблему наявності розриву між семантикою юриста і оперативною семантикою програміста, яка може призвести до неприйнятних операційних і нормативних ризиків, звертає увагу ряд авторів [4], що також може бути причиною суперечок при реалізації розумного контракту у вигляді програмного забезпечення. Необхідність вирішення спорів збільшує для всіх сторін як вартість окремих контрактних транзакцій, так і вартість контракту в цілому.

Слід зауважити, що причини для деяких суперечок від самого початку закладаються в традиційні контракти завдяки застосуванню категорій, які неоднозначно визначаються і сприймаються, таких як: “відповідають прийнятим стандартам”, “відповідно до прийнятих правил”, “сумлінна практика”, “розумний строк” тощо. Це відбувається, як правило, внаслідок того, що юристи недостатньо ретельно підходять до написання текстів контрактів або недостатньо ретельно опрацьовують його положення. Переклад контрактів (алгоритму контракту) з природної мови в машинну (комп’ютерну програму) закономірно призводить до необхідності або точного опису таких категорій чи інших термінів, або їх заміни іншими категоріями чи термінами, які точно і однозначно сприймаються, або виключення таких категорій з тексту контракту. А це, в цілому, тільки покращує правові умови виконання контрактів роблячи їх більш

прозорими і логічними, що призводить до зменшення ризиків збільшення вартості контрактних транзакцій за рахунок виникнення суперечок.

Ідентифікація та аналіз джерел і причин збільшення вартості контрактних транзакцій повинні скласти окремий предмет правових досліджень, результати якого можуть позитивно вплинути на широту застосування розумних контрактів.

Залежно від складності конкретної контрактної діяльності комп’ютерні програмні та/або програмно-апаратні засоби, за допомогою яких реалізуються розумні контракти, можуть набувати складної структури і мати багато тисяч рядків виконуваних машинних кодів. В цьому випадку готова програмна реалізація, можливо, буде працювати не так як це проектувалося її розробниками, тобто результати її роботи не відповідатимуть алгоритму контракту. Крім того, у величезному масиві програмних кодів вірогідна поява механічних помилок, які не завжди можуть проявлятися в процесі налагодження програми. Один з яскравих прикладів – це операційна система Windows, поновлення до якої, викликані необхідністю усунення помилок, виходять практично щотижня.

Вважають, що будь-який розумний контракт з тисячами умов і вкладених операторів перемикання типу “якщо..., то..., інакше...” може бути протестований для кожної умови або кожного оператора перемикання, наявного в комп’ютерній програмі, що виконує контракт, тобто аналогічно тому, як розробники програмного забезпечення “налагоджують” свій власний код, перевіряючи його у всіх можливих обставинах, юристи зможуть перевіряти контракти, даючи кожній стороні угоди більш чітке розуміння свого ризику [5].

Тому існує необхідність створення правових механізмів реагування на випадки неправильного виконання контракту внаслідок наявності помилок в програмному забезпеченні, які можуть бути виявлені на будь-якому етапі життєвого циклу розумного контракту.

В цілому, можна визнати, що перетворення алгоритму дій, який відображається в традиційному контракті, у відповідну комп’ютерну програму представлятиме один з основних бар’єрів на шляху широкого поширення розумних контрактів в різних сегментах соціуму.

Отже, вважаємо за доцільне створення в майбутньому систем автоматизації програмування розумних контрактів, зрозумілих для використання юристами без наявності спеціальної освіти в програмуванні. Для цього необхідно провести дослідження з розробки предметно-орієнтованих на юридичну сферу надвисокорівневих мов програмування з високим рівнем абстракції [16] або програмування природньою мовою з використанням штучного інтелекту [19; 20], в тому числі, можливо, і з використанням рекурентної нейронної мережі [7].

При виконанні розумного контракту можуть мати місце випадки необхідності скасування контракту, наприклад, тому, що його було укладено під примусом або за інших обставин, які традиційне договірне право визнає підставою для невизнання контракту. Деякі автори вважають, що, імовірно, незворотні транзакції можуть бути просто компенсовані подальшою транзакцією, що приводить все до початкового стану [1].

Очевидно, таке припущення викликано розумінням того, що ретельно складений і алгоритмізований контракт після переведення його на одну з мов програмування зажадає значних зусиль для його оперативної зміни. Однак, цілком можлива розробка алгоритмів, досить гнучких до зміни умов, але це вимагатиме реалізації інноваційних підходів.

Інший приклад, який ілюструє необхідність забезпечення можливості внесення змін до розумного контракту, пов’язаний з використанням технології блокчейна в управлінні ланцюгами поставок, що тягне за собою серйозні проблеми для правового

регулювання. Такі правила, як європейська директива про нефінансову звітність, можуть вплинути на використання ланцюжків блокчейна в процесі поставок, оскільки при цьому від компаній вимагається розкриття достовірної інформації з екологічних питань, соціальних аспектів та аспектів роботи співробітників, дотримання прав людини та вимог щодо боротьби з корупцією з метою підвищення прозорості їх діяльності. Однак відсутність посередника на більшості або всіх етапах ланцюжка поставок в майбутньому може створити невизначеність для залучених сторін, особливо коли мова йде про автоматизовані форми виконання та нагляду за транзакціями. У більшості випадків необхідно враховувати поняття та механізми юридичної відповідальності або юридичної відповідальності при виникненні непередбачених проблем тому, що якщо вони не враховані, то контракт повинен бути допрацьований [11].

Створення юридичних і технологічних можливостей для внесення змін в розумні контракти шляхом зміни програмного забезпечення може бути також обумовлено тим, що в процесі розгляду спорів або оцінки відповідності змісту контракту вимогам законодавства суди можуть виносити рішення про зміну умов виконання розумного контракту або навіть про визнання недійсним договору (стаття 215 ЦКУ).

Однією з важливих проблем застосування розумних контрактів є правозастосовність та можливість розгляду спорів в суді [2]. Це обґрунтовується тим, що багато галузей, де можливе використання розумних контрактів, наприклад, галузь фінансових послуг, мають досить детальне правове регулювання, в тому числі, яке передбачає наявність для учасників угод спеціальних ліцензій та дозволів.

Крім того, на наш погляд, потрібно приділити серйозну увагу питанням, пов’язаним з розглядом суперечок в суді, наприклад, питанням юридичної фіксації та протоколювання всіх зовнішніх чинників, що впливають на виконання контракту в автоматичному режимі, можливості проведення експертизи на відповідність комп’ютерної програми алгоритму виконання контракту, який вона реалізує тощо.

Для розгляду спору в суді, як і для багатьох інших випадків, які сьогодні передбачаються традиційною системою права, необхідна наявність тексту розумного контракту, викладеного природньою юридичною мовою. Таким чином, необхідна правова регламентація трансляції (перекладу) комп’ютерної програми, що містить опис розумного контракту, природньою юридичною мовою. Правові механізми регулювання такої трансляції можуть бути аналогічні існуючим правовим механізмам здійснення перекладу з іноземних мов.

Розгляд в суді суперечок, пов’язаних з розумними контрактами, завжди буде знаходитися на стику проблем, пов’язаних з правовим регулюванням, і проблем їх інтерпретації в лексиці програм, “зрозумілих” обчислювальним машинам, а також проблем відповідності алгоритмів програмного забезпечення алгоритмам правового регулювання.

Тому закономірно виникає питання про необхідність формування корпусу суддів, що повинні володіти відповідними компетенціями для розгляду спорів, обтяжених застосуванням комп’ютерних технологій, і наявності інституту кваліфікованих експертів.

Особливу увагу для випадку застосування розумних контрактів в технологіях Інтернету речей слід приділити питанням взаємодії мережевих комп’ютерних програмних та/або програмно-апаратних засобів, за допомогою яких реалізуються розумні контракти, з фізичними або цифровими об’єктами, зміна стану яких буде виступати своєрідним тригером (спусковим механізмом) для вступу в дію тих чи інших положень контракту. В цьому випадку будуть мати місце проблеми правового регулювання верифікації фізичних або цифрових об’єктів, забезпечення кібербезпеки технологічних систем

взаємозв’язку зовнішніх об’єктів з розумними контрактами, підтвердження достовірності та цілісності, а також протоколювання переданих повідомлень. Крім того, виникають проблеми правового визначення юридичних механізмів анонімізації фізичних об’єктів з метою забезпечення захисту персональних даних.

Ще один ймовірний суттєвий бар’єр у взаємодії розумних контрактів з фізичними або цифровими об’єктами було визначено в одній з робіт, в якій зазначається, що кожен вузол в ланцюжку блокчейнів виконує розумні контракти незалежно (вірніше, дублюючи їх), але не синхронно, тому, коли виникає необхідність використання інформації від зовнішнього джерела, то кожен вузол робить це повторно і окремо [15]. Автори роботи стверджують, що оскільки це джерело знаходиться поза блокчейн-ланцюгом, то немає гарантії, що кожен вузол отримає одну і ту саму інформацію, оскільки фізичні або цифрові об’єкти можуть в різний час генерувати різну інформацію про свій стан або стати тимчасово недоступними. Наявність відмінностей в інформації, яка записується в вузли блокчейн-ланцюжка, призводить до відмови в транзакції, тобто у відмові виконання якихось положень розумного контракту. Ця проблема вимагає вирішення як на технологічному, так і на правовому рівні.

При використанні розумних контрактів питання забезпечення кібербезпеки стають пріоритетними, як і для всіх технологій, заснованих на використанні ІКТ та мережі Інтернет. У 2016 році Децентралізована автономна організація (Decentralized Autonomous Organization, DAO) оголосила, що хакер використав уразливість в Ethereum-платформі, що використовує блокчейн, завдавши загальний збиток близько 150 мільйонів доларів. Але недолік був не в самій платформі блокчейна, а в наявності лазівки в коді розумного контракту, тому хакеру вдалося створити рекурсивну відправку грошей в контракті, тобто команда відправки коштів викликала інший запит “відправити гроші” [6].

Незважаючи на те, що в даному конкретному випадку платформа, яка використовує блокчейн, виявилася поза підозрою, питання забезпечення надійності її функціонування залишається відкритим. Як інфраструктурна основа для багатьох додатків розумного контракту, вона повинна відповідати підвищеним вимогам до надійності, безперервності і стійкості роботи, а також до стійкості в умовах реалізації кіберзагроз.

Відомо, що кожен вузол в блокчейн-мережі зберігає величезні обсяги одних і тих самих даних і, в залежності від застосування блок-ланцюга, деякі з цих даних можуть бути класифіковані як персональні дані, що створює певні труднощі із застосуванням законодавства в частині недопущення несанкціонованої та незаконної обробки персональних даних і недопущення їх випадкової втрати або знищення, а також в частині задоволення законної вимоги про їх видалення [8].

З урахуванням того, що в цілому технології Інтернету речей при наданні послуг і проведенні робіт будуть характеризуватися превалюванням горизонтальних зв’язків між суб’єктами, особливої актуальності набуває вивчення проблеми можливості використання розумних контрактів в транскордонному режимі. Розумні контракти, що базуються на використанні блокчейн-платформ, максимально підходять для підтримки горизонтальних взаємозв’язків між суб’єктами договірних відносин і дозволяють здійснювати транзакції в транскордонному режимі, що призводить до необхідності вирішення проблеми визначення юрисдикції цих контрактів.

З входженням в життя соціуму нових технологій, в тому числі і інформаційних, практично завжди виникає питання про реакцію системи права на використання цих технологій в суспільних відносинах. Традиційно ця реакція зводиться до чотирьох варіантів: нічого не треба змінювати; потрібні лише деякі косметичні зміни в праві і

законодавстві; необхідні, іноді суттєві, зміни положень традиційної системи права і законодавства; створення нових галузей права і законодавства.

Вельми спокусливим виглядає четвертий варіант, який, здавалося б, створює умови для реалізації можливості креативно та інноваційно підійти до вирішення проблем правового регулювання суспільних відносин, які виникають у зв’язку з використанням нових технологій. В останні роки такий підхід набув поширення у вигляді пропозицій про створення нових галузей права, наприклад таких як: право електронних магістралей, телекомунікаційне право, право ІТ, комп’ютерне право тощо. Звичайно, подібні ідеї мають право на життя, але за умови: по-перше, серйозного теоретичного обґрунтування можливості виділення окремої нової галузі права, по-друге, обґрунтування практичної та економічної доцільності.

Нові технології широко входять в практику суспільних відносин – це, як правило, проривні технології, що ведуть до прогресу в розвитку соціуму. З урахуванням сучасної динамічності розвитку суспільних та економічних процесів, часу на створення систем правового регулювання з урахуванням використання цих нових технологій відводиться не дуже багато. З іншого боку, відсутність ефективної системи правового регулювання є одним з основних бар’єрів на шляху широкого використання нових технологій в суспільних відносинах, що може бути причиною зниження темпів економічного розвитку.

Тому для багатьох сучасних стратегій розвитку системи права в зв’язку з появою нових технологій, наприклад, технологій Інтернету речей або розумного контракту, та їх використання для реалізації суспільних відносин найбільш ефективним є третій варіант: внесення необхідних змін в традиційну систему права і систему законодавства.

У частині розумних контрактів слід підтримати позицію Сабо Н., яка кореспондується з нашим попереднім висновком: “успіх загального права контрактів в поєднанні з високою вартістю його заміни робить доцільним як збереження, так і використання принципів цього права там, де це необхідно” [10].

Таким чином, в частині вирішення проблеми формування правового забезпечення широкого застосування розумних контрактів з урахуванням викладеного раніше і результатів деяких досліджень [10; 11] можна сформувати наступні завдання, що стоять перед правою наукою:

1. Інтеграція системи правового регулювання застосування розумних контрактів, що буде розроблятись, в традиційну національну правову систему.

2. Визначення юридичного статусу розумного контракту, формування правових вимог до його форми і змісту.

3. Визначення юрисдикції розумних контрактів, в тому числі, за наявності транскордонних транзакцій.

4. Дослідження особливостей правовідносин, пов’язаних з розумними контрактами, юридичних прав, обов’язків і відповідальності його сторін.

5. Дослідження проблеми визначення юридичних ризиків та обмежень використання розумних контрактів в різних сферах застосування.

6. Формування правових механізмів нагляду, встановлення відповідальності за порушення умов розумного контракту і відшкодування завданих збитків або за наявності помилок в комп’ютерній програмі.

7. Формування правових вимог щодо забезпечення достовірності індикації та фіксації подій або явищ в реальному світі, факт наявності яких є причиною для здійснення певних дій сторін при виконанні розумного контракту.

8. Розв’язання правовими засобами проблеми наявності неповної можливості для учасників договору спостерігати за всіма прихованими діями програмного забезпечення розумного контракту, що може призвести до небажаного збитку.

9. Розробка правових механізмів верифікації сторін контракту, що здійснюють транзакцію, на момент її здійснення.

10. Розв’язання протиріччя між законодавчими вимогами обмеження доступу до персональних даних та іншої чутливої інформації сторін контракту, яка в ньому може міститися, і відкритістю інформації за всіма транзакціями для всіх учасників публічної децентралізованої мережі блокчейнів і її зберіганням в кожному вузлі блокчейн-ланцюжка.

11. Правова регламентація забезпечення кібербезпеки як програмного забезпечення, що підтримує використання розумних контрактів, так і програмно-апаратних платформ, на яких розміщується це програмне забезпечення.

12. Розробка пропозицій стосовно процесуальних особливостей розгляду в суді суперечок, пов’язаних з розумними контрактами.

Висновки.

1. Розумні контракти – прогресивна форма контрактів, що створює умови для реалізації на практиці багатьох переваг, що обумовлюється використанням технологій Інтернету речей.

2. Розумні контракти – інноваційна форма контрактів, укладення, виконання та припинення яких відбувається з використанням мережевих комп’ютерних програмних та/або програмно-апаратних засобів, що мають взаємозв’язок з фізичними або цифровими об’єктами, за участю або без участі людини, що вимагає проведення системних і комплексних правових досліджень в рамках цивільного, фінансового та інформаційного права.

3. З метою зменшення невизначеності та вартості впровадження правового регулювання використання розумних контрактів доцільно орієнтуватися на стратегію яка полягає в максимально можливому використанні правових механізмів традиційної системи права з необхідним удосконаленням або розвитком окремих правових положень. До створення нових правових конструкцій слід вдаватися тільки в тому випадку, коли в існуючому законодавстві не знаходиться навіть віддаленої аналогії.

Використана література

1. A. Liou. Using Bitcoin’s Blockchain Technology In Legal Practice. March 28, 2016. URL : http://stlr.org/2016/03/28/using-bitcoins-blockchain-technology-in-legal-practice/ (дата звернення : 26.09.2017).

2. B. Cant. Smart Contracts in Financial Services: Getting from Hype to Reality. Capgemini Consulting. Digital Transformation Institute. URL : https://www.capgemini.com/consulting/resources/blockchain-smart-contracts/ (дата звернення : 26.09.2017).

3. Bitcoin. Wikipedia. URL : https://en.wikipedia.org/wiki/Bitcoin (дата звернення : 26.09.2017).

4. F. Al Khalil, M. Ceci, L. O’Brien, T. Butler. A Solution for the Problems of Translation and Transparency in Smart Contracts. February 2017. URL : http://www.grctc.com/wp-content/uploads/2017/06/GRCTC-Smart-Contracts-White-Paper-2017.pdf (дата звернення : 26.09.2017).

5. J. Stark. How Close Are Smart Contracts to Impacting Real-World Law? Apr 11, 2016. URL : https://www.coindesk.com/blockchain-smarts-contracts-real-world-law/ (дата звернення : 26.09.2017).

6. K. Panetta. Why Blockchain’s Smart Contracts Aren’t Ready for the Business World. June 26, 2017. URL : http://www.gartner.com/smarterwithgartner/why-blockchains-smart-contracts-arent-ready-for-the-business-world (дата звернення : 26.09.2017)

7. L. Mou, R. Men, G. Li, L. Zhang, Z. Jin. On End-to-End Program Generation from User Intention by Deep Neural Networks. 25 Oct 2015. URL: https://arxiv.org/pdf/1510.07211v1.pdf (дата звернення : 26.09.2017).

8. L. Russell. Training & knowledge Features and articles Blockchains: The legal landscape. 5 December 2016. URL : https://www.blakemorgan.co.uk/training-knowledge/features-and-articles/blockchains-legal-landscape/ (дата звернення : 26.09.2017).

9. M. Raskin. The Law and Legality of Smart Contracts. April 2017. URL : https://www.georgetownlawtechreview.org/the-law-and-legality-of-smart-contracts/GLTR-04-2017 (дата звернення : 26.09.2017).

10. N. Szabo, Smart Contracts: Building Blocks for Digital Markets, 1996. URL : http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html (дата звернення : 26.09.2017).

11. P. Boucher, S. Nascimento, M. Kritiko. How blockchain technology could change our lives. In-depth Analysis. EPRS, European Parliament. February 2017. URL : http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_IDA%282017%29581948 (дата звернення : 26.09.2017).

12. P. De Filippi, S. Hassan. Blockchain technology as a regulatory technology: From code is law to law is code. First Monday. Volume 21, Number 12. December 2016. URL : http://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 (дата звернення : 26.09.2017).

13. S. Hourani. Cross-Border Smart Contracts: Boosting International Digital Trade through Trust and Adequate Remedies. URL : http://www.uncitral.org/pdf/english/congress/Papers_for_Programme/11-HOURANI-Cross-Border_Smart_Contracts.pdf (дата звернення : 26.09.2017).

14. Smart Contracts. Dream Team Investments. May 15 2017. URL: https://medium.com/@research15/smart-contracts-871160e7feac (дата звернення: 26.09.2017).

15. Smart contracts. Strafford Kent Law. Nottingham. August 12, 2017. URL : http://www.straffordkentlaw.co.uk/blog/smart-contracts/ (дата звернення : 26.09.2017).

16. Very high-level programming language. URL : https://en.wikipedia.org/wiki/Very_high-level_programming_language (дата звернення : 26.09.2017).

17. Булгаков И. “Умные” контракты и современное договорное право. – (Декабрь 25, 2016). URL : https://theferma.media/smart-contracts-and-deals (дата звернення : 26.09.2017).

18. Ивкушкин К., Вашкевич А. Горизонты умных контрактов. Открытые системы. / СУБД. – 2017. – № 03. – (22.08.2017). URL : https://www.osp.ru/os/2017/03/13052706 (дата звернення: 26.09.2017).

19. Программирование на естественном языке. – (2011-10-24). URL : http://www.pegasus-project.org/ru/Dobro_pozalovat.html (дата звернення : 26.09.2017).

20. Программные инструкции на естественном языке, или интенциональное программирование. – (8 октября 2015). URL : https://habrahabr.ru/post/268401 (дата звернення : 26.09.2017).

21. Савельев А.И. Договорное право 2.0 : “умные” контракты как начало конца классического договорного права // Вестник гражданского права. – 2016. – № 3. – С. 32-60. URL: https://elibrary.ru/item.asp?id=26468044 (дата звернення : 26.09.2017).

22. Rob Preston. Larry Ellison Introduces ‘A Big Deal’ : The Oracle Autonomous Database. Oct 2017. URL: https://www.oracle.com/features/oracle-open-world-2017-keynote/ellison-1/index.html (дата звернення : 26.09.2017).

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

УДК 340.132 [001.18+335.078+608.1]

ДОРОНІН І.М., *кандидат юридичних наук, доцент,*
завідувач наукової лабораторії
НДІ інформатики і права НАПрН України

РОЗВИТОК ЕМЕРДЖЕНТНИХ (НОВІТНІХ) ТЕХНОЛОГІЙ ТА РЕГУЛЮВАННЯ У ЦІЙ СФЕРІ ЯК РЕАЛІЗАЦІЯ ФУНКЦІЙ ДЕРЖАВИ

Анотація. *У статті досліджено проблеми розвитку емерджентних технологій та особливостей державного регулювання у цій сфері. Визначено поняття “емерджентної технології” у контексті правового регулювання. Проаналізовано стан реалізації функції держави за допомогою права стосовно відносин у сфері використання емерджентних технологій.*

Ключові слова: *новітні технології, емерджентність, емерджентні технології, правове регулювання, державне регулювання, регуляторна діяльність, функції держави.*

Summary. *The article explores the problems of development of emerging technologies and features of state regulation in this sphere. The concept of “emerging technology” is defined in the context of legal regulation. The realization of the state function through the law concerning the relations arising in sphere of use of emerging technologies is analyzed.*

Keywords*: emerging technologies, legal regulation, state regulation, regulation, state functions.*

Аннотация. *В статье исследованы проблемы развития эмерджентных технологий и особенностей государственного регулирования в этой сфере. Определено понятие “эмерджентной технологии” в контексте правового регулирования. Проанализировано состояние реализации функции государства через право по поводу отношений, возникающих в сфере использования эмерджентных технологий.*

Ключевые слова*: новейшие технологии, эмерджентность, эмерджентные технологии, правовое регулирование, государственное регулирование, регуляторная деятельность, функции государства.*

Постановка проблеми. Правові проблеми, що виникають у зв’язку із розвитком технологій постійно перебували у полі зору юридичної науки. Основні дослідження з цієї проблематики у вітчизняній науці відбувались навколо питань сфери цивільного права (договірне та зобов’язальне право щодо створення та експлуатації об’єктів-результатів науково-дослідної роботи), господарського права (правове регулювання господарської діяльності у сфері науки і техніки), дещо меншою мірою – інших галузей права.

Водночас, загальнотеоретичні і соціальні аспекти розвитку технологій, його вплив на стан правового регулювання суспільних відносин залишались поза увагою науковців, що за радянських часів зумовлювалося відповідним ідеологічним впливом. Філософські аспекти науково-технічного прогресу, а також розвитку технологій розглядались суто через призму положень діалектичного матеріалізму. Правові ж аспекти регламентації суспільних відносин в СРСР розглядались як складова державного управління.

У подальшому проблематика досліджень змінювалась і через постійні зміни у загально-філософських підходах науковців до цього явища. Розвиток інформаційної сфери, створення інформаційного суспільства, соціальні трансформації під впливом факторів глобалізації зумовили і зміни у ставленні до суті та змісту правового регулювання відносин, які пов’язані з розвитком технологій.

Результати аналізу наукових публікацій. Питання правової регламентації окремих аспектів нових (на той час) технологій у вітчизняній правовій науці досліджувались, починаючи з 1960-х років, як правило у зв’язку з правовими проблемами народного господарства та у контексті відповідних положень договірного права. Насамперед мова йде про роботи В.О. Рассудовського, М.П. Рінга, Ч.Н. Азімова [1 – 3]. У подальшому у сфері уваги науковців знаходились питання правового статусу наукових працівників, особливостей регламентації фінансового забезпечення наукових робіт та управління науковими установами. У цьому контексті варто виділити дослідження В.А. Дозорцева, В.П. Рассохіна, Ч.Н. Азімова та інших [4 – 7]. Окрім цього, ґрунтовні розробки проводились у сфері правових аспектів винаходів та раціоналізаторської діяльності та пов’язаних із цим питань захисту прав інтелектуальної власності.

Зміна світоглядних підходів до розуміння науково-технічного прогресу і введення в науковий обіг нової термінології – “інновацій” та “інноваційного розвитку” зумовило і зміну характеру досліджень науковців у сфері правової науки. У цьому аспекті слід виділити праці О.Сімсон [8], О. Сердюкової [9], В. Фурашева [10], О. Шевердіної [11] та інших.

Сплеск інтересу науковців до означеної проблематики зумовлений законодавчими новаціями, що є складовими правового забезпечення державної політики інноваційного розвитку України. Зокрема, 4 липня 2002 року Верховною Радою України було прийнято Закон України “Про інноваційну діяльність”, 25 червня 2009 року – Закон України “Про наукові парки”, а 8 вересня 2011 року – Закон України “Про пріоритетні напрями інноваційної діяльності в Україні”. Задекларована законодавцем мета правового регулювання визначена у преамбулі останнього з них як “забезпечення інноваційної моделі розвитку економіки шляхом концентрації ресурсів держави на пріоритетних напрямах науково-технічного оновлення виробництва, підвищення конкурентоспроможності вітчизняної продукції на внутрішньому і зовнішньому ринках”.

Останні наукові дослідження у сфері правового забезпечення використання новітніх технологій за кордоном насамперед зосереджені навколо їх регуляторного аспекту. У цьому контексті доцільно виділити працю М. Фенвіка, В. Каала та Е. Вермюллена [12] щодо перспектив державного (у тому числі правового) регулювання відносин у сфері новітніх технологій.

Але слід зазначити, що питання розвитку технологій та їх співвідношення з правом у контексті реалізації функцій держави вітчизняними іноземними науковцями практично не розглядались.

Метою статті є дослідження проблемних питань правового регулювання суспільних відносин у сфері застосування новітніх технологій, ролі держави у їх регулюванні та визначення основних напрямів наступних досліджень.

Виклад основного матеріалу. Традиційний підхід до правових питань новітніх технологій у часи колишнього СРСР полягав у їх вивченні та дослідженні насамперед у контексті управління. Але оскільки система управління в СРСР та соціалістичних державах характеризувалася насамперед адміністративно-командною моделлю зазначене повною мірою стосується і сфери науково-технічного розвитку [13, с. 176-177].

Окрім цього, державна політика у сфері науково-технічного прогресу чітко характеризувалась впливом політичного фактору – саме у рішеннях з’їздів КПРС формулювались загальні настанови та основні завдання, які реалізовувались державними органами. Такий підхід чітко свідчив про ідеологічне та політичне

підґрунтя у питанні стратегічного планування державної політики, а її правове забезпечення здебільшого стосувалось питань регулювання окремих аспектів управління у цій сфері.

На стратегічному рівні адміністративно-командні методи управління під партійним керівництвом зумовлювали відставання СРСР саме у розвитку новітніх технологій, тобто таких технологій, які виникали у нових сферах і ґрунтувались на наукових відкриттях. У питанні реалізації виробництва технологій прикладного (у першу чергу оборонного) призначення зазначений підхід у цілому був достатньо ефективним за умови належного фінансування.

У подальшому після розпаду СРСР питання правового забезпечення розвитку новітніх технологій відчували з одного боку вплив притаманних соціалізму підходів у державному регулюванні цієї сфери, які залишались в управлінській культурі незалежної України, а з іншого – очевидним було відставання права як регулятора відносин у суспільстві від процесу трансформації усього суспільства, що було зумовлено розвитком і впровадженням таких технологій.

Насамперед, слід визначитись які саме технології, що є новітніми у хронологічному сенсі, здійснюють істотний вплив на суть і характер суспільних відносин сучасного суспільства. У науковій літературі для цих явищ вживаються насамперед терміни “науково-технічна революція”, “науково-технічний прогрес”, “новітні технології”, “інновації”. Зокрема, стаття 1 Закону України “Про інноваційну діяльність” визначає інновації як “новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери”, а інноваційну діяльність як “діяльність, що спрямована на використання і комерціалізацію результатів наукових досліджень та розробок і зумовлює випуск на ринок нових конкурентоздатних товарів і послуг”. Якщо проаналізувати приписи статті 4 Закону України “Про пріоритетні напрями інноваційної діяльності в Україні”, що безпосередньо визначає стратегічні пріоритетні напрями на період до 2021 року, то інноваційну діяльність по суті можливо визначати як створення та використання певних технологій.

Для англомовної наукової літератури більш розповсюдженим є термін “emerging technologies”. Зазначений термін зазвичай перекладається як “новітні технології”, що безумовно не відображає його зміст. На думку сучасних дослідників зазначені технології мають наступні основні властивості – радикальну новизну, відносно швидке зростання, узгодженість, значний вплив та невизначеність [14, с. 37].

Тобто для такої технології характерна стрибкоподібність – вона з’являється нібито нізвідки, хоча ґрунтуються на відповідних наукових концепціях. Якщо проаналізувати розвиток технологій, пов’язаних із використанням графену, то легко встановити, що ці дослідження провадились хіміками та фізиками протягом 100 років, допоки у 2004 році не відбувся прорив у науці – винайдення методу отримання графену науковцями Манчестерського університету А. Геймом та К. Новосьоловим, за що у 2010 році вони отримали Нобелівську премію з фізики. Їхні праці створили теоретичне підґрунтя для численних наукових досліджень прикладного характеру та розвитку технологій застосування графену в промисловості та енергетиці. Таким чином, за останні 10 років відбувається стрибкоподібне зростання технологій використання графену в різних сферах.

Значний вплив технології зумовлює її використання у найрізноманітніших сферах людської діяльності. Наприклад, запропонований свого часу вид технології розподіленої обробки даних, що став відомий як “блокчейн”, може бути використаний не лише для

створення і застосовування альтернативних грошових одиниць, які не емітує держава, але і для зберігання різноманітної критично важливої інформації з гарантією захисту від знищення, втручання та змін, що має значення для різноманітних сфер – від державних реєстрів до генних досліджень.

На нашу думку в науковій літературі доцільно використовувати термін “емерджентний” стосовно найменування таких технологій. Зокрема у сучасній українській мові існує термін “емерджентний” насамперед як філософський термін що визначає появу чогось нового (нових якостей), що зумовлено втручанням ідеальних сил [15, с. 224]. Існує розуміння “емерджентності” у теорії систем як поява у цілого “властивостей, неадитивних властивостям частин, що входять у нього, тобто властивостей, які не витікають з властивостей його частин”. [16, с. 94]. Як вважає О. Гребешкова емерджентність є наслідком прояву, як мінімум, трьох факторів: “1) різкого нелінійного посилення раніше малопомітної властивості; 2) наслідком непередбачуваної біфуркації якої-небудь підсистеми; 3) наслідком рекомбінації зв’язків між елементами” [17, с. 133].

Зазначене розуміння, що вживається у теорії систем, може бути загалом сприйнятим, хоча і не повністю відображає властивості емерджентності стосовно технологій, що було визначено Д. Ротоло, Д. Хікс і Б. Мартіном.

Тому під “емерджентною технологією”, у контексті розгляду питань правового регулювання відповідних суспільних відносин, пропонується розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями, яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед.

За таких умов правова регламентація планування у цій сфері зводиться до правового забезпечення державної політики стосовно науково-технічного розвитку і навряд чи буде адекватною стану суспільних відносин.

На це свого часу було звернуто увагу в літературі у контексті дослідження проблематики “інноваційного права” та визначення його місця у системі права. Зокрема, О.Сімсон пропонувала визнати, що “інноваційні відносини” (а мова йде саме про правовідносини щодо використання технологій) мають “двоїсну публічно-правову природу” [8, с. 82]. Тобто такі правовідносини поєднують у собі приватно та публічно-правовий характер.

З урахуванням стрибкоподібного характеру розвитку, що притаманний для емерджентних технологій, на сьогодні можливо лише визначити доволі приблизний перелік таких технологій. Зокрема, зазвичай до них відносять “мікро-літальні апарати” (MAV, різновид некерованих літальних апаратів малих розмірів), “об’ємний друк” (комп’ютерний 3D-друк, клейтроніка, наноассемблер), технології на основі використання фулеренів та графену, біометрія, “гнучка електроніка” тощо.

Що стосується правового регулювання суспільних відносин у контексті застосування емерджентних технологій, то зазначене розглядалось насамперед з точки зору відповідного урядування та державного регулювання. Потреба в державному регулюванні цієї сфери виникає насамперед як відповідь суспільному запиту на безпеку. Першим питанням, яке потребує невідкладного вирішення, є питання безпеки (заборони на заподіяння шкоду та ефективне і швидке відшкодування), а отже з точки зору теорії права мова йде про юридичну відповідальність. У другій частині питання у повному обсязі можуть бути застосовані загальні положення цивільного права. Що стосується державних заборон, то ситуація у цій сфері не настільки однозначна.

Науковцями цілком вірно було визначено, що регуляторний вплив стосовно технологій та науки у багатьох випадках здійснити досить складно беручи до уваги обмежений характер інформації щодо ситуації [12, с. 9]. Емерджентна технологія ґрунтується на вже існуючих і має безпосереднє призначення, але має стрибкоподібний характер, що призводить до неможливості визначати наперед сферу застосування, а це обмежує заходи регламентації.

У сучасних економічно розвинутих країнах мета регуляторного впливу держави полягає у досягненні насамперед мети належного функціонування вільного ринку та вільної економіки, що стосується фінансової, банківської сфери, біржової торгівлі, зв’язку, транспорту, тощо. При цьому регуляторні органи, як правило, не є органами державного управління, що прямо підпорядковані урядам, а формуються на паритетних засадах за законодавчо визначеною процедурою. Беручи до уваги таку схему державного регулювання, питання його традиційного здійснення у фінансовій сфері або у біржовій торгівлі не викликає складнощів, оскільки відповідним фахівцям відома уся можлива інформація стосовно технологій, які застосовуються, та інші відомості, що здійснюють вплив на ринок. Інша річ – це новітні технології у фінансовій сфері. Очевидно, що у питанні застосування криптовалют регуляторний вплив у більшості країн здійснюється із значним запізненням, оскільки складність проблем, які породжені застосуванням емерджентної технології “блокчейн”, виходить далеко за традиційні рамки уявлень про фінансовий ринок, а стрибкоподібний характер технології зводить нанівець усі існуючі механізми регулювання станом “на сьогодні”.

На нашу думку, в питаннях правової регламентації використання емерджентних технологій слід спиратись на розуміння державного регулювання як реалізації відповідних функцій держави. Попри досить великий обсяг наукової літератури із зазначеного питання, погляди на сутність функцій держави зумовлені традиційним у вітчизняній правовій науці розумінням функцій держави як основних напрямів її діяльності [18, с. 136; 19, с. 118].

Але традиційно існували та існують інші погляди. Зокрема, Г. Єллінек, використовуючи термін “функції держави”, розуміє їх як відповідні напрями розподілу функцій державної влади – “законодавства, виконання (управління) та відправлення правосуддя” [20, с. 576]. Так само розумів функції держави і Г. Кельзен [21, с. 318]. Практично аналогічним чином розуміють функції держави і сучасні західні юристи. У концептуальних поглядах на суть державного регулювання, що притаманний європейській і американській правовій науці, сутність регулювання розуміється насамперед у контексті реалізації функцій правосуддя, тобто правоохоронної діяльності. У такому разі діяльність із регулювання фондового ринку спрямована на недопущення вчинення кримінальних правопорушень (шахрайства, зловживання тощо), а також встановлення монополізму та інших ускладнень вільному ринку. Саме у такому контексті регулювання визначається і ставлення держави щодо обмежень у розповсюдженні певних технологій.

Наприклад, у ситуації із державними обмеженнями стосовно криптографічного захисту інформації мета таких обмежень полягала у недопущенні використання криптографії терористичними та організованими злочинними угрупованнями. Розповсюдження відкритих програмних засобів складного шифрування призвело до того, що зашифровані повідомлення не могли бути відкриті та прочитані правоохоронними органами. Намагання встановити певні обмеження щодо вільного розповсюдження таких програм призвело до бурхливої дискусії у засобах масової інформації, а також судових процесів між громадськими активістами у сфері захисту

приватності та державними органами. Як зазначила одна із громадських організацій – Фундація досліджень інформаційної політики (FIPR) у своєму маніфесті від 25 травня 2005 року “криптографічна війна” з урядом вважається закінченою у зв’язку із прийняттям Урядом США відповідних заходів з послаблення режиму обмежень доступу до криптографічних засобів. Суть спору, який тривав з початку 1970-років полягала у обмеженні стосовно проведення досліджень у сфері стійких криптографічних ключів недержавними установами та приватними особами, а також щодо розповсюдження таких технологій поза межами державних органів і установ. Зазначена проблема виникла після вільного розповсюдження у глобальній комп’ютерній мережі першої програми стійкого шифрування PGP, що викликало подальший судовий процес американських правоохоронних органів щодо її розробника Ф. Ціммермана та кампанії захисників громадянських прав прихильників приватності. Зазначене завершилось ослабленням державного впливу, а самі події увійшли в історію під назвою “криптографічних воєн” [22 с. 339-344, 348-349, 353-355]. Сама по собі криптографічна технологія стійких шифрів не є емерджентною, але саме вона стала підґрунтям для справді емерджентної технології – “блокчейну”.

Повертаючись до державного регулювання емерджентних технологій у контексті реалізації функції держави, слід визначити низку основних ключових моментів.

По-перше, мова повинна йти про забезпечення реалізації основної функції держави – загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії, насамперед стосовно заздалегідь деструктивних технологій. Основна проблема полягає у неочевидності деструктивності і можливих помилок в оцінці суті технологій. Так, на сьогодні, склалася досить неоднозначна ситуація із правовими обмеженнями у сфері використання технологій генної модифікації. Широка кампанія проти генно-модифікованих організмів спирається на не до кінця встановлені факти, а уявно випереджувальна функція правових норм заборони може лише загальмувати технологічний прогрес в окремих державах.

По-друге, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності, як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції.

По-третє, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності. На жаль у чинному вітчизняному законодавстві норми стосовно розвитку інноваційної діяльності а також відповідні заохочення багато у чому мають суто декларативний характер.

Зазначене дозволяє прийти до наступних загальних висновків.

Висновки.

1. Розвиток сучасних технологій і характер наукових досліджень чітко визначає певну специфіку в суспільних відносинах, які пов’язані з використанням таких технологій. Зазначена специфіка відносин зумовлена швидким стрибкоподібним характером розвитку технологій і значно ускладнює будь-яке, у тому числі державне регулювання у цій сфері.

2. Зазначені технології може бути виокремлено під найменуванням емерджентних технологій. Під “емерджентною технологією” у контексті розгляду питань правового регулювання відповідних суспільних відносин пропонується розуміти таку технологію, що є радикально новою, швидкозростаючою, узгодженою з існуючими технологіями,

яка при цьому здійснює значний вплив на суспільне життя у різноманітних сферах, які неможливо передбачити наперед.

3. У питанні правового регулювання як реалізації функцій держави слід виходити насамперед з загальної безпеки суспільства, особливо це стосується правових норм, що забороняють певні дії – зокрема, стосовно заздалегідь деструктивних (руйнівних) технологій. Основна проблема полягає у неочевидності деструктивності і можливих помилок в оцінці суті технологій, тому пошук можливих шляхів вирішення зазначеної низки проблем є перспективним для подальших досліджень у галузі правової науки.

Окрім цього, регулювання державою відносин стосовно використання емерджентних технологій має обмежуватися реалізацією економічної функції держави, яка полягає у забезпеченні економічної багатоманітності як це визначено у ст. 15 Конституції України. Мова повинна йти про заохочення вільного ринку і державний вплив на недопущення зловживання монопольним станом та обмеження економічної конкуренції. Водночас, надання різноманітних пріоритетів та преференцій повинно бути обґрунтованим і випливати із реально існуючої необхідності.

Використана література

1. Рассудовский В.А. Договор на выполнение проектных и изыскательских работ в капитальном строительстве / В.А. Рассудовский. – М. : Изд-во АН СССР, 1963. – 160 с.

2. Азимов Ч.Н. Предмет договорных обязательств в области научно-технического прогресса // Проблемы социалистической законности. – 1978. – Вып. 3. – С. 25-32.

3. Дозорцев В.А. Законодательство и научно-технический прогресс / В.А. Дозорцев. – М. : Юрид. лит., 1978 – 191 с.

4. Азимов Ч.Н. Классификация договорных обязательств в области научно-технического прогресса // Проблемы социалистической законности. – 1980. – Вып. 6. – С. 62-68.

5. Право и управление научными организациями / [В.А.Рассудовский, В.П. Рассохин, Г.А.Лахтин и др.]. – М. : Наука, 1980. – 343 с.

6. Ринг М.П. Хозрасчетная система создания и внедрения новой техники / М.П. Ринг. – М. : Наука, 1982. – 335 с.

7. Рассохин В.П. Механизм внедрения достижений науки. Политика, управление, право / В.П. Рассохин. – М. : Наука, 1985. – 286 с.

8. Сімсон О. Інноваційне право як запорука сталого інноваційного розвитку // Теорія і практика інтелектуальної власності. – 2010. – № 4. – С. 81-86.

9. Сердюкова О. Основні проблеми правового забезпечення інноваційного розвитку територій // Державне управління та місцеве самоврядування. – 2013. – Вип. 1(16). – С. 255-264.

10. Фурашев В.М. Питання інформатизації – питання інноваційного розвитку // Право та інноваційне суспільство. – 2013. – № 1. – С. 5-17. – Режим доступу : http://apir.org.ua/wp-content /uploads/2014/11/furashev_ua.pdf. – Назва з екрана. – Дата звернення : 29.11.2017 р.

11. Шевердіна О.В. Правове забезпечення інноваційних процесів як фактор реформування економіки // Право та інноваційне суспільство. – 2014. – № 1(2). – С. 22-29. – Режим доступу : http://apir.org.ua/wp-content/uploads/2014/11/Sheverdina.pdf. – Назва з екрана. – Дата звернення : 29.11.2017 р.

12. Fenwick Mark. Regulation Tomorrow : What Happens When Technology is Faster then the Law? / Mark Fenwick, Wulf Kaal, Erik Vermeulen – TILEC Discussion Paper, October 2016.

13. Пономарева С.А. Особенности научно-технической политики социалистических стран на примере СССР и ЧССР (1965-1990 гг). // Вопросы экономики и права. – 2012. – № 7. – С. 176-179.

14. Rotolo Daniele. What Is Emerging Technology? / Daniele Rotolo, Diana Hicks, Ben R. Martin – Working Paper of Science Policy Research Unit. University of Sussex. – February 2015. – 46 p.

15. Нечволод Л. Сучасний словник іншомовних слів / Л. Нечволод – Х. : Торсинг-Плюс, 2009. – 768 с.

16. Геселева Н.В. Емерджентні властивості системи / Н.В. Геселева, Н.М. Заріцька / Бізнес Інформ. – 2013. – № 7. – С. 93-97.

17. Гребешкова О.М. Емерджентність у стратегічному процесі підприємства // Формування ринкової економіки : зб. наукових праць. – 2009. – Вип. 22. – С. 129-137.

18. Сурилов А.В. Теория государства и права / А.В. Сурилов. – К.: Вища школа, 1989. – 439 с.

19. Кельман М.С. Загальна теорія держави і права : підручник. – К. : Кондор, 2005. – 314 с.

20. Еллинек Г. Общее учение о государстве / Г. Еллинек – СПб. : Юридический центр Пресс, 2004. – 752 с.

21. Кельзен Г. Чисте правознавство / Г. Кельзен – К., Юніверс, 2004. – 496 с.

22. Сингх С. Книга шифров. Тайная история шифров и их расшифровки / С. Сингх. – М. : АСТ-Астрель, 2007 – 477 с.

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

УДК 519.6+625.1

КАЧИНСЬКА К.А., аспірант Інституту телекомунікацій
і глобального інформаційного простору НАН України,
ВАРИЧЕВА Д.І., студент ТІ НТУУ “КПІ” ім. І. Сікорського,
СВИРИДЕНКО С.В., студент ФТІ НТУУ “КПІ” ім. І. Сікорського

ІНТЕРНЕТ-ТЕХНОЛОГІЇ: ОЦІНКА ПРІОРИТЕТНОСТІ МАНІПУЛЮВАННЯ СВІДОМІСТЮ ЗА ДОПОМОГОЮ МЕТОДІВ РАНЖУВАННЯ

Анотація. *У статті розглянуті основні сучасні інформаційні технології маніпуляції свідомістю. За допомогою системної методології ранжування отримані кількісні оцінки пріоритетів зазначених сугестивних технологій. Здійснено порівняльний аналіз методів ранжування та оцінок пріоритетності способів маніпулювання свідомістю за допомогою методів Акоффа-Черчмена, Неймана-Моргенштерна та Фішберна.*

Ключові слова: *інформаційні технології, маніпулювання свідомістю, сугестія, кількісні оцінки пріоритетів, методи Акоффа-Черчмена, Неймана-Моргенштерна, Фішберна.*

Summary: *The article discusses the main modern information technologies for consciousness manipulation. The quantitative estimates of these suggestive technologies priorities are obtained with the help of system ranking methodology. A Comparative Analysis of Ranking Methods and priority ranking of methods for manipulating consciousness is carried out using the following methods: the Churchman-Ackoff method, the Neumann-Morgenstern method and Fishburn's Method.*

Keywords: *information technologies, consciousness manipulation, suggestion, quantitative evaluation* of *priorities, the Churchman-Ackoff method, the Neumann-Morgenstern method and Fishburn's Method.*

Аннотация. *В статье рассмотрены основные современные информационные технологии манипуляции сознанием. С помощью системной методологии ранжирования получены количественные оценки приоритетов упомянутых суггестивных технологий. Осуществлен сравнительный анализ методов ранжирования и оценок приоритетности способов манипулирования сознанием с помощью методов Акоффа-Черчмена, Неймана-Моргенштерна и Фишберна.*

Ключевые слова: *информационные технологии, манипулирование сознанием, суггестия, количественные оценки приоритетов, методы Акоффа-Черчмена, Неймана-Моргенштерна, Фишберна.*

Постановка проблеми. Попри те, що дослідження такого складного явища, як використання сугестивних технологій для негативного впливу на психіку людини здійснюються давно, тема маніпулювання свідомістю вийшла далеко за межі наукових досліджень. Враховуючи “гібридний” характер сучасних війн, вона розширила не лише рамки публічної дискусії, але й набула вкрай важливого практичного значення – убачається глобальна можливість переходу від відкритого збройного протистояння армій до методів ведення прихованої війни.

Дослідженню методів сугестивних технологій присвячена велика кількість публікацій [5; 6; 7; 16], одначе останнім часом дедалі більшого значення набуває проблема застосування сучасних Інтернет-технологій для маніпулювання свідомістю особи, суспільства та держави [8; 13; 15].

У роботах [6; 9; 16] були розглянуті переваги використання Інтернету для здійснення маніпулятивного впливу, а також виділені сучасні найбільш поширені Інтернет-технології, що використовуються для маніпуляції свідомістю. У першу чергу серед них мають розглядатися: *електронна пошта*, *мережеве теле- та радіомовлення*, *електронні видання*, *спеціальні мережеві сайти*, *боти*, *чати*, *онлайн-форуми*, *іміджборди*, *блоги*, *смартмоби*, *комп’ютерні ігри*, *електронна психотронна зброя*, *соціальні мережі*.

У той час серед сучасних методів маніпуляції свідомістю, на нашу думку, найбільш актуальними є наступні: *метод “ствердження”* (M_1), *метод “дезінформація”* (M_2), *метод “фокусу на емоції”* (M_3), *метод “використання стереотипів”* (M_4), *метод “повтору інформації”* (M_5), *метод “міфів”* (M_6), *метод “створення проблем”* (M_7), *метод “закидання брудом”* (M_8), *метод “відволікання уваги”* (M_9), *метод “історичних аналогій”* (M_{10}) [6; 10; 16].

Розв’язання задачі оцінки пріоритетів різних методів сугестивного впливу для окремих Інтернет-технологій маніпулювання свідомістю (альтернатив), зважаючи на її складність і багатокритеріальність, потребує використання багатьох системних методів ранжування [1; 2].

Метою статті є дослідження основних інформаційних технологій маніпулювання свідомістю, а також їх ранжування за допомогою кількісних оцінок пріоритетів, здійснення порівняльного аналізу різних методів ранжування та оцінок пріоритетності способів маніпулюванні свідомістю, отриманих за допомогою методів Акоффа-Черчмена, Неймана-Моргенштерна та Фішберна.

Виклад основного матеріалу. При ранжуванні об’єктів різної природи, у першу чергу, враховують факт різноманіття проявів будь-якої властивості, що утворюють множину елементів які перебувають в певних логічних відношеннях між собою. Особливості цих відношень, визначають особливості відповідних їм шкал вимірювання [2; 14]. Тому нині ранжування розглядають як спосіб оцінки об’єктів у порядковій шкалі, коли кожному з них приписується місце в послідовності об’єктів.

З типом шкали тісно пов’язані способи обробки і результати вимірювань, у тому числі ті, що стосуються негативного впливу на свідомість людини. Для ранжування складних об’єктів часто залучають експертів, які на основі знань і досвіду упорядковують їх в порядку переваги, керуючись одним або декількома вибраними показниками порівняння. Залежно від виду відносин можливі різні варіанти їх ранжування [4].

У роботі розглядається строге ранжування методів сугестії, пов’язаних з різними технологіями маніпулювання свідомістю людини, методи Акоффа-Черчмена, Неймана-Моргенштерна та Фішберна, враховуючи при цьому, що серед об’єктів між собою немає еквівалентів. У даному випадку між об’єктами існує тільки відношення строгого порядку.

У результаті порівняння всіх об’єктів згідно відношення строгого порядку складається упорядкована послідовність $a_1 > a_2 > ... > a_N$, де об’єкт з першим номером є найкращим з усіх об’єктів, об’єкт з другим номером менш бажаний, ніж перший об’єкт, але краще всіх інших об'єктів і т.д. Отримана система об’єктів із відношенням строгого порядку, за умови порівнянності всіх об’єктів, утворює повний строгий порядок. Для чого доведено існування числової системи, елементами якої є дійсні числа, пов’язані між собою відношенням нерівності [3; 12]. Тобто упорядкування об’єктів відповідає впорядкування чисел $x_1 >...> x_N$, де $x_i = \varphi(a_i)$. Можлива і зворотна послідовність, в якій найкращому об’єкту приписується найменше число, а у напрямку зниження переваги об’єктам приписуються великі числа.

Ранжування сугестивних методів за допомогою підходу Акоффа-Черчмена. Вперше даний метод був запропонований для кількісних оцінок результатів соціологічних досліджень, що дало можливість не тільки упорядкувати задану множину альтернатив, але й наближено вказати силу переваги. При досить сильних вимогах до вагових коефіцієнтів вимірювання, вони можуть бути переведені у розряд більш сильних шкал [1; 3], що означає суттєву модифікацію процедури упорядкування.

Щодо оцінки альтернатив, то в гуманітарних науках даний метод є одним з найбільш популярних методів ранжування об’єктів. Він передбачає послідовне коригування оцінок, вказаних експертами. Основні припущення, на яких заснований метод Акоффа-Черчмена, полягають в наступному [3; 12]:

- кожній альтернативі a_i, (i = 1,…, n) ставиться у відповідність дійсне невід’ємне число $\varphi(a_i)$;
- якщо альтернатива a_i більш прийнятна за альтернативу a_j, то $\varphi(a_i) > \varphi(a_j)$; якщо ж альтернативи a_i і a_j рівноцінні, то $\varphi(a_i) = \varphi(a_j)$;
- якщо $\varphi(a_i)$ і $\varphi(a_j)$ – оцінки альтернатив a_i і a_j, то $\varphi(a_i) + \varphi(a_j)$ відповідає спільному здійсненню альтернатив a_i і a_j. Останнє припущення про адитивність оцінок альтернатив є найбільш сильним.

Згідно з методом Черчмена-Акоффа альтернативи ранжуються за перевагою. Нехай для зручності викладу альтернатива a_1 найбільш прийнятна, за нею йде a_2 і так далі. Експерт вказує попередні чисельні оцінки $\varphi(a_i)$ для кожної з альтернатив. Іноді найбільш прийнятній альтернативі приписується оцінка 1, інші оцінки розташовуються між 0 і 1 відповідно до їх переваги. Потім експерт робить порівняння альтернативи a_1 і суми альтернатив $a_2,...,a_n$. Якщо a_1 більш прийнятна, то експерт коригує оцінки так, щоб $\varphi(a_1) > \sum_{i=2}^{n} \varphi(a_i)$. Інакше повинна виконуватися нерівність $\varphi(a_1) \leq \sum_{i=2}^{n} \varphi(a_i)$.

Якщо альтернатива a_1 виявляється менш прийнятною, то для уточнення оцінок вона порівнюється за перевагою з сумою альтернатив $a_2,...,a_{n-1}$. Після того, як альтернатива a_1 виявляється більш прийнятною за суму альтернатив $a_2,...,a_k$, вона виключається з розгляду, а замість оцінки альтернативи a_1 розглядається і коригується оцінка альтернативи a_2. Процес триває до тих пір, поки відкоригованими не виявляться оцінки усіх альтернатив.

Результати розрахунків наведені у Таблиці 1.

Таблиця 1

Оцінки ранжування сугестивних методів, отримані за допомогою підходу Акоффа-Черчмена

Засоби Інтернет-комунікації	M_1	M_2	M_3	M_4	M_5	M_6	M_7	M_8	M_9	M_{10}
Електронна пошта	0,2	1	0,85	0,25	0,95	0,7	0,1	0,6	0,35	0,1
Мережеве теле- та радіомовлення	0,75	0,15	0,5	0,25	0,65	0,45	0,05	0,9	1	0,3
Електронні видання	0,95	0,7	0,6	0,85	0,15	0,4	0,35	1	0,2	0,45
Спеціальні мережеві сайти	1	0,85	0,6	0,45	0,1	0,5	0,75	0,3	0,05	0,35
Боти	0,45	0,95	0,75	0,2	1	0,8	0,5	0,15	0,3	0,1
Чат	0,75	0,7	0,45	1	0,4	0,55	0,8	0,2	0,25	0,1
Онлайн-форуми	0,7	0,75	0,55	0,4	0,65	0,95	0,3	1	0,25	0,15
Іміджборд	0,3	0,45	0,5	0,8	0,65	0,15	1	0,05	0,9	0,1

Блоги	0,95	0,7	0,35	0,5	0,8	0,15	0,3	1	0,1	0,55
Смартмоб	0,9	0,3	1	0,4	0,8	0,75	0,55	0,2	0,25	0,05
Комп’ютерні ігри	0,45	0,7	0,55	1	0,35	0,1	0,5	0,85	0,2	0,8
Психотронна зброя	0,6	0,45	1	0,65	0,95	0,15	0,8	0,2	0,85	0,25
Соціальні мережі	0,9	0,85	0,55	0,65	0,1	1	0,6	0,2	0,5	0,4

Ранжування сугестивних методів за допомогою підходу Неймана-Моргенштерна. Суть даного методу полягає в отриманні числових оцінок альтернатив за допомогою так званих імовірнісних сумішей [11; 12]. Основу методу становить припущення, згідно з яким експерт для будь-якої альтернативи a_j менш переважної, ніж a_i, але більш переважної, ніж a_l , може вказати число a_p ($0 \leq p \leq 1$) таке, що альтернатива a_j еквівалентна змішаній альтернативі (ймовірнісної суміші) $[pa_i, (1-p)a_l]$.

Суть змішаної альтернативи полягає в тому, що альтернатива a_i вибирається з ймовірністю p, в той час коли альтернатива a_l з імовірностю $(1-p)$. Очевидно, що коли p досить близько до 1, то альтернатива a_j є гіршою, ніж змішана альтернатива $[pa_i, (1-p)a_l]$.

Водночас розглядається система припущень (аксіом) про властивості змішаних і незмішаних альтернатив. До числа таких припущень відносяться аксіома про зв'язність і транзитивність відношення переваги альтернатив, аксіома про те, що змішана альтернатива $[pa_i, (1-p)a_l]$ краща ніж $[p'a_i, (1-p')a_l]$, якщо $p > p'$ та ін.

Якщо зазначена система переваг виконується, то для кожної зі сукупності основних альтернатив $a_1, a_2,...,a_N$ визначаються числа $x_1, x_2,...,x_N$, що характеризують чисельну оцінку змішаних альтернатив.

Чисельна оцінка змішаної альтернативи $[p_1a_1, ..., p_Na_N]$ дорівнює $p_1x_1 + ... + p_Nx_N$. Змішана альтернатива $[p_1a_1, p_2a_2,..., p_Na_N]$ переважніша за змішану альтернативу $[p'_1a_1, p'_2a_2,..., p'_Na_N]$, якщо $p_1x_1 + p_1x_1 +...+ p_Nx_N > p'_1x_1 + ... + p'_Nx_N$.

Таким чином, встановлюється існування функції корисності $x_1p_1 + ... + x_Np_N$, значення якої характеризує ступінь перевагу будь-якої змішаної альтернативи, зокрема і незмішаної. Більш переважна та змішана альтернатива, для якої значення функції корисності більше.

Результати розрахунків наведені у Таблиці 2.

Таблиця 2

Оцінки ранжування сугестивних методів, отримані за допомогою підходу Неймана-Моргенштерна

Засоби Інтернет-комунікації	**M_1**	**M_2**	**M_3**	**M_4**	**M_5**	**M_6**	**M_7**	**M_8**	**M_9**	**M_{10}**
Електронна пошта	0,02	0,23	0,03	0,21	0,19	0,11	0,1	0,06	0,04	0,01
Мережеве теле- та радіомовлення	0,14	0,03	0,11	0,05	0,12	0,09	0,01	0,16	0,22	0,07
Електронні видання	0,15	0,12	0,09	0,14	0,01	0,06	0,05	0,28	0,02	0,08
Спеціальні мережеві сайти	0,25	0,21	0,13	0,06	0,02	0,07	0,17	0,03	0,01	0,05
Боти	0,09	0,13	0,11	0,05	0,27	0,12	0,1	0,04	0,07	0,02
Чат	0,13	0,11	0,09	0,18	0,085	0,1	0,16	0,055	0,075	0,015
Онлайн-форуми	0,13	0,16	0,05	0,04	0,08	0,22	0,03	0,26	0,02	0,01
Іміджборд	0,07	0,09	0,1	0,15	0,13	0,05	0,18	0,04	0,17	0,02
Блоги	0,16	0,14	0,6	0,11	0,15	0,02	0,04	0,19	0,01	0,12
Смартмоб	0,17	0,07	0,21	0,08	0,14	0,12	0,1	0,04	0,05	0,02

Комп’ютерні ігри	0,09	0,12	0,11	0,16	0,04	0,03	0,1	0,15	0,06	0,14
Психотронна зброя	0,08	0,07	0,2	0,01	0,17	0,11	0,14	0,02	0,16	0,04
Соціальні мережі	0,21	0,15	0,08	0,11	0,01	0,25	0,1	0,02	0,04	0,03

Ранжування сугестивних методів за допомогою підходу Фішберна. Метод оцінки пріоритетності показників Фішберна відноситься до сукупності системних методів ранжування [2]. Алгоритм реалізації методу наступний:

- *крок 1*. Особа, яка приймає рішення (ОПР), ранжує окремі методи маніпуляції свідомістю в порядку їх важливості, тобто застосовується порядкова шкала пріоритетності;

- *крок 2*. Для кожної з наведених вище Інтернет-технологій коефіцієнти пріоритетності показників B_k розраховуються за формулою:

$$B_k = \frac{2(K+1-l_k)}{K(K+1)},$$

де K – кількість методів сугестивного впливу для Інтернет-технологої маніпулювання свідомістю; l_k – номер (ранг) k -го методу сугестивного впливу в порядку його важливості. При цьому виконується умова нормування:

$$\sum_{i=1}^{K} B_k = 1$$

Результати розрахунків наведені у Таблиці 3.

Таблиця 3

Оцінки ранжування сугестивних методів, отримані за допомогою підходу Фішберна

Засоби Інтернет-комунікацій	**M_1**	**M_2**	**M_3**	**M_4**	**M_5**	**M_6**	**M_7**	**M_8**	**M_9**	**M_{10}**
Електронна пошта	0,055	0,182	0,145	0,091	0,164	0,127	0,018	0,109	0,036	0,073
Мережеве теле- та радіомовлення	0,145	0,036	0,109	0,055	0,127	0,091	0,018	0,164	0,182	0,073
Електронні видання	0,073	0,127	0,109	0,182	0,055	0,018	0,091	0,164	0,036	0,145
Спеціальні мережеві сайти	0,182	0,164	0,127	0,091	0,036	0,109	0,145	0,055	0,018	0,073
Боти	0,091	0,164	0,127	0,055	0,182	0,145	0,109	0,036	0,073	0,018
Чат	0,145	0,127	0,091	0,182	0,073	0,109	0,164	0,036	0,055	0,018
Онлайн-форуми	0,127	0,145	0,091	0,073	0,109	0,164	0,055	0,182	0,036	0,018
Іміджборд	0,073	0,091	0,109	0,145	0,127	0,055	0,182	0,018	0,164	0,036
Блоги	0,164	0,127	0,073	0,091	0,145	0,036	0,055	0,182	0,018	0,109
Смартмоб	0,164	0,073	0,182	0,091	0,145	0,127	0,109	0,036	0,055	0,018
Комп’ютерні ігри	0,073	0,127	0,109	0,182	0,055	0,018	0,091	0,164	0,036	0,145
Психотронна зброя	0,091	0,073	0,182	0,109	0,164	0,018	0,127	0,036	0,145	0,055
Соціальні мережі	0,164	0,145	0,091	0,127	0,018	0,182	0,109	0,036	0,073	0,055

Яким методом кількісної оцінки пріоритетів різних способів маніпулювання свідомістю користуватися – загалом залежить від навику і звички. Всі розглянуті методи можна застосовувати для вирішення зазначеної задачі. Одначе оцінки пріоритетів відрізняються не тільки величиною, але й кількістю математичних операцій їх розрахунку. Тому для оцінки ефективності застосування кожного методу сугестії розглянемо результати їх застосування для оцінки пріоритетів.

Метод “ствердження”. Є видом психологічного впливу, що здійснюється через електронні засоби масової комунікації у спосіб ведення пропаганди. Як показують розрахунки, метод “ствердження” є найбільш ефективним для наступних Інтернет-ресурсів: *спеціальні мережеві сайти, електронні видання, блоги, смартмоби, соціальні мережі, мережеве теле- та радіомовлення*, *чати*, *онлайн форуми*. Очевидно, що метод маніпулювання свідомістю становить найбільшу загрозу як засіб утвердження в суспільстві певних цінностей (оцінку пріоритетів див. Рис. 1).

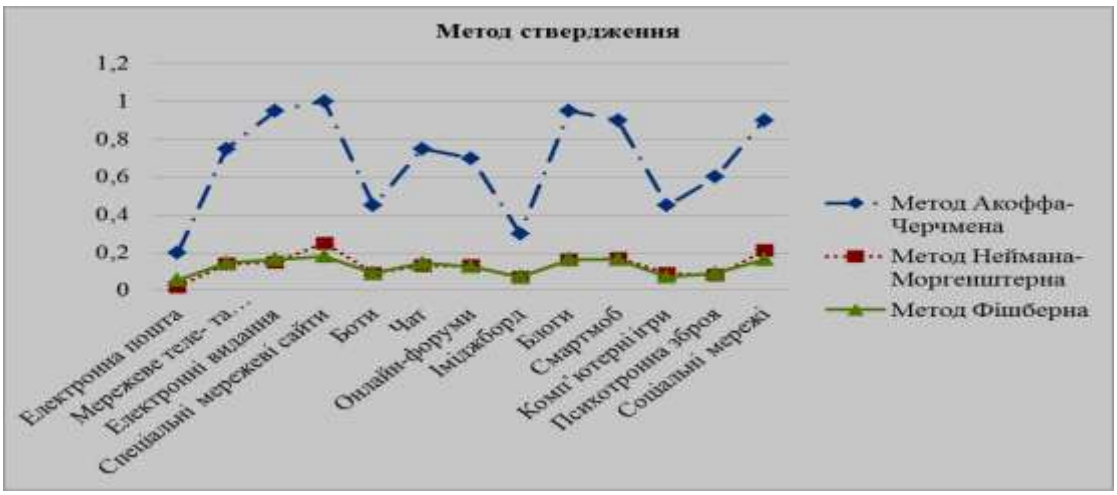

Рис. 1. Оцінки пріоритетів для методу “ствердження”.

Метод “дезінформація”. Ми розглядаємо дезінформацію як обман, спосіб психологічного впливу на людину, в основі якого є надання інформації, що вводить її в оману щодо правдивого стану справ. Як показали розрахунки, метод **“**дезінформація**”** – досить грубий, але ефективний прийом маніпулювання масовою свідомістю. Сила його в тому, що він опирається на такі Інтернет-ресурси, як: *електронна пошта, боти, спеціальні мережеві сайти, соціальні мережі, онлайн-форуми, чати, електронні видання, блоги комп’ютерні ігри*. Враховуючи, що заходи з дезінформування здійснюються за єдиним задумом з ретельним узгодженням пропорцій правди і брехні (при максимальному використанні правдоподібної інформації), з обов’язковим викривленням істинних намірів, цілей і завдань, то його можна сміливо розглядати як один з основних інструментів маніпуляції свідомістю (оцінку пріоритетів див. Рис. 2).

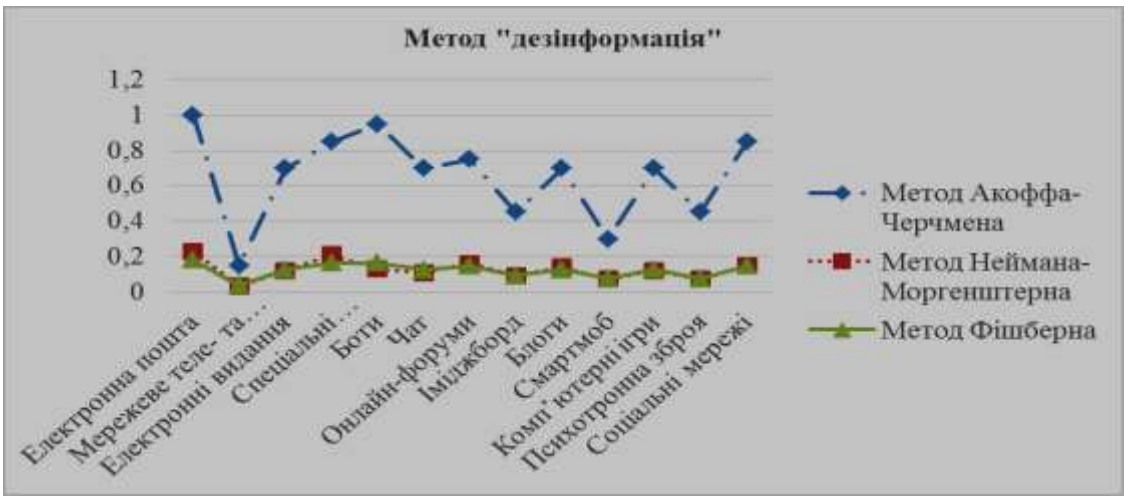

Рис. 2. Оцінки пріоритетів для методу “дезінформація”.

Метод “фокусу на емоції”. Розглядають як спосіб створення у широкої аудиторії певного настрою з одночасною передачею їй пропагандистської інформації. Він дозволяє перехопити емоційну сферу людини за рахунок зняття психологічного захисту, яку вона вибудовує на розумовому рівні, свідомо намагаючись захиститися від пропагандистського “промивання” мозку. Таким чином, метод “фокусу на емоції”, поєднуючи телевізійні, телефонні, комп’ютерні та інші лінії зв’язку, соціальні мережі, призводить до пробудження у об'єкта впливу намірів, що змінюють його бажання, настрої, поведінку, погляди тощо.

Метод “фокусу на емоції” найбільш ефективний для таких Інтернет-ресурсів, як: *смартмоб, психотронна зброя, електронна пошта, боти.* Якщо вважати, що пропагандистський вплив на людину відбувається на емоційному рівні, поза її свідомим контролем, і при цьому ніякі раціональні контраргументи не спрацьовують, то даний метод можна віднести до числа найбільш простих і ефективних технологій маніпуляції свідомістю (оцінку пріоритетів див. Рис. 3).

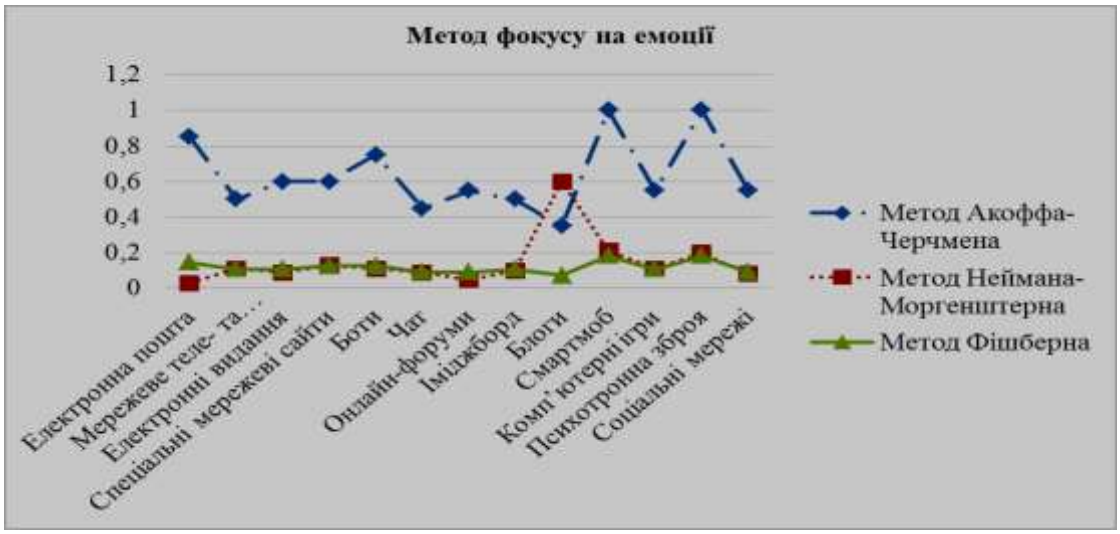

Рис. 3. Оцінки пріоритетів для методу “фокусу на емоції”.

Метод “використання стереотипів”. Використання технологій інформаційно-психологічного впливу для маніпулювання громадською думкою – поширене у світі явище. До числа таких технологій відноситься метод “використання стереотипів”, теоретичні засади якого становить концепція спрощення. Цю концепцію виснував ще на початку XX століття відомий американський політичний оглядач В. Ліппман. Він вважав, що процес сприйняття – це приєднання ще невідомого явища до вже існуючого у свідомості стереотипу. Тому преса має стандартизувати те, про що повідомляє, до зрозумілих стереотипів і усталених думок. У свою чергу спрощення тісно пов’язане зі створенням стереотипів. Текст стає доступним тоді, коли його зміст тільки підтверджує усталені в суспільстві стереотипи. Створивши ж сенсацію, можна замовчати багато важливих деталей та навіть подати недостовірну інформацію.

За цим правилом лежить психологічне твердження, що людина підсвідомо тяжіє до простих пояснень складних проблем. Тому нині серед Інтернет-технологій психологічного впливу на людину, що ґрунтуються на методі “використання стереотипів”, найбільш популярними є наступні: *чати, комп’ютерні ігри, електронні видання, іміджборди, психотронна зброя, соціальні мережі*. Частіше за все головним

методом закріплення потрібних стереотипів у свідомості людини вони обирають повторення (оцінку пріоритетів див. Рис. 4).

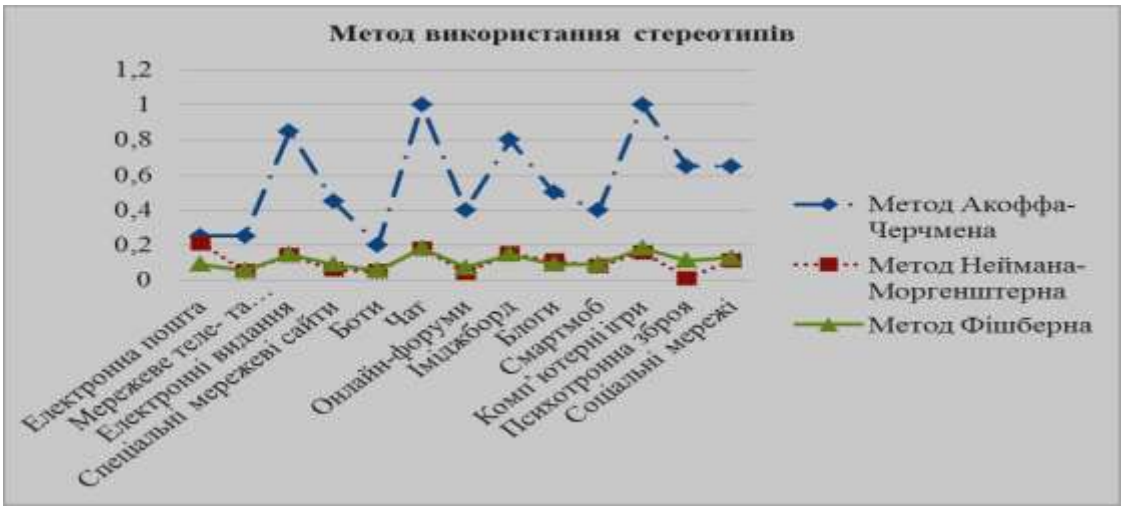

Рис. 4. Оцінки пріоритетів для методу “використання стереотипів”.

Метод “повтору інформації”. Одним з найефективніших способів пропаганди є безустанне повторення одних і тих самих тверджень, щоб до них звикли і стали сприймати не розумом, а на віру. Тому традиційні ЗМІ часто використовували повтори в повідомленнях новин, де в кожному наступному випуску найбільш значуща інформація повторювалася без будь-яких коригувань або змін.

Нині метод “повтору інформації” поширився й на електронні ЗМІ. Серед них найбільш ефективними є *боти, електронна пошта, психотронна зброя, блоги, смартмоби, онлайн-форуми, іміджборди, мережеве теле- та радіомовлення*. Вони досконало оволоділи технікою “повтору”, часто вживаючи різні гасла та ключові слова. При цьому, повторення засвоюються людьми як очевидні, що не потребують доказів (оцінку пріоритетів див. Рис. 5).

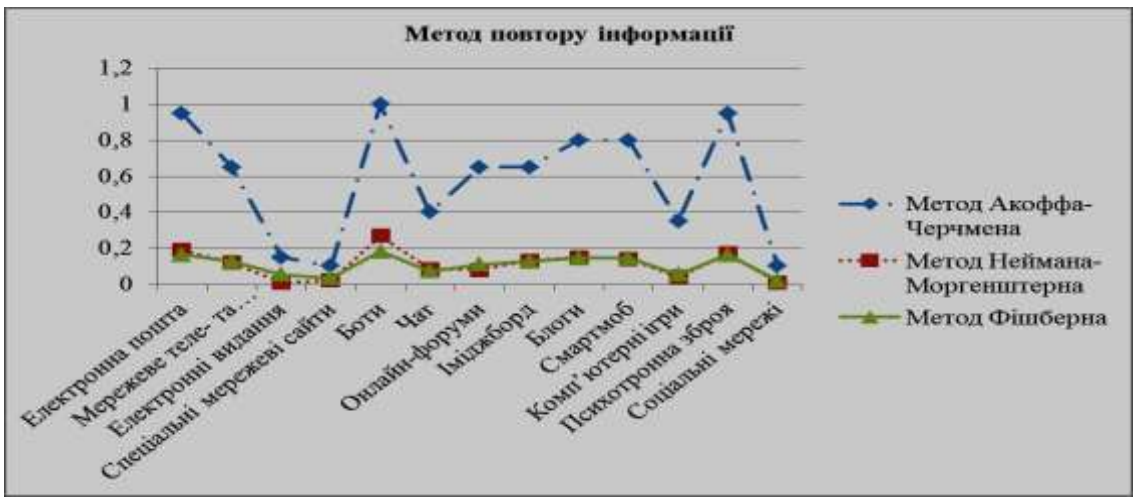

Рис. 5. Оцінки пріоритетів для методу “повтору інформації”.

Метод “міфів”. Основою будь-якого маніпулювання масовою свідомістю є соціальний міф – твердження чи ідеї, які сприймаються переважно на віру, без будь-якого критичного осмислення [5; 15]. Метод “міфів”, узагалі як усяке маніпулювання, тісно пов’язаний із цілеспрямованим перекручуванням інформації, що передбачає використання

багатого арсеналу конкретних методів впливу на свідомість людей. Подібне її перетворення є потужним інструментом при створенні маніпулятивних технологій.

Нині для укорінення соціальних міфів серед Інтернет-технологій маніпулювання найбільш поширеними є: *соціальні мережі, онлайн-форуми, боти, смартмоб, електронна пошта* (оцінку пріоритетів див. Рис. 6).

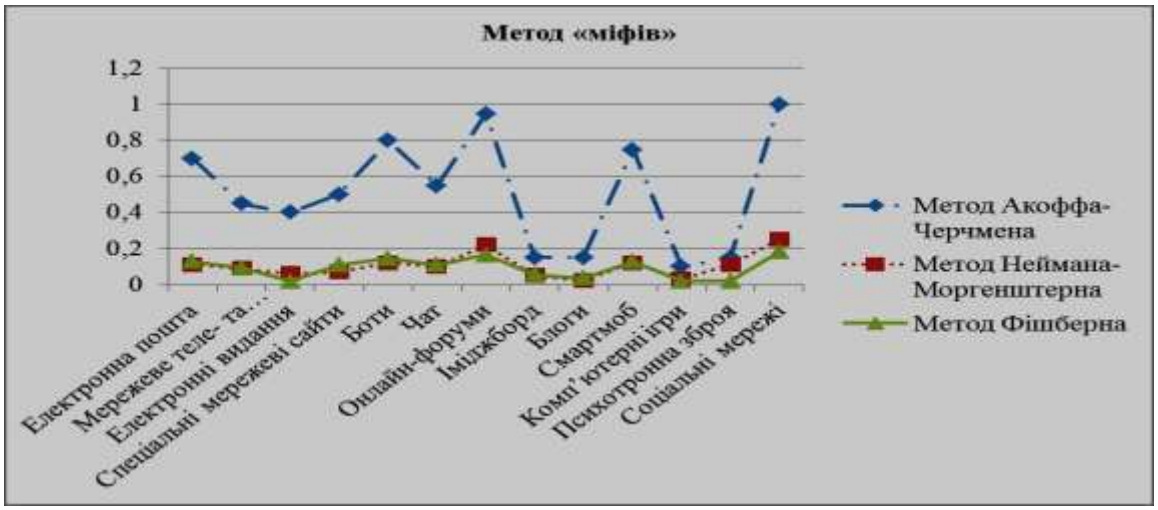

Рис. 6. Оцінки пріоритетів для методу “міфів”.

Метод “створення проблем”. Через ускладнення соціально-економічних і соціально-політичних відносин, посилення протиріч у суспільстві людині дедалі складніше стає розібратися у тому, що коїться довкола. Метод “створення проблем” є ефективним інструментом маніпуляції людською свідомістю, в першу чергу, з боку влади [5; 7]. Цей метод також називається “проблема – реакція – рішення”: створюється проблема, що викликає необхідну реакцію і дозволяє впровадити рішення, які в іншій ситуації викликали би супротив (наприклад – криваві теракти, як рушій для прийняття законів, що підсилюють “безпеку”, а по суті діють на обмеження звичайних громадян).

Особливо сильно ефект “проблема – реакція – рішення” проявляє себе для таких Інтернет-ресурсів, як: *іміджборд, психотронна зброя, чати, спеціальні мережеві сайти* (оцінку пріоритетів див. Рис. 7).

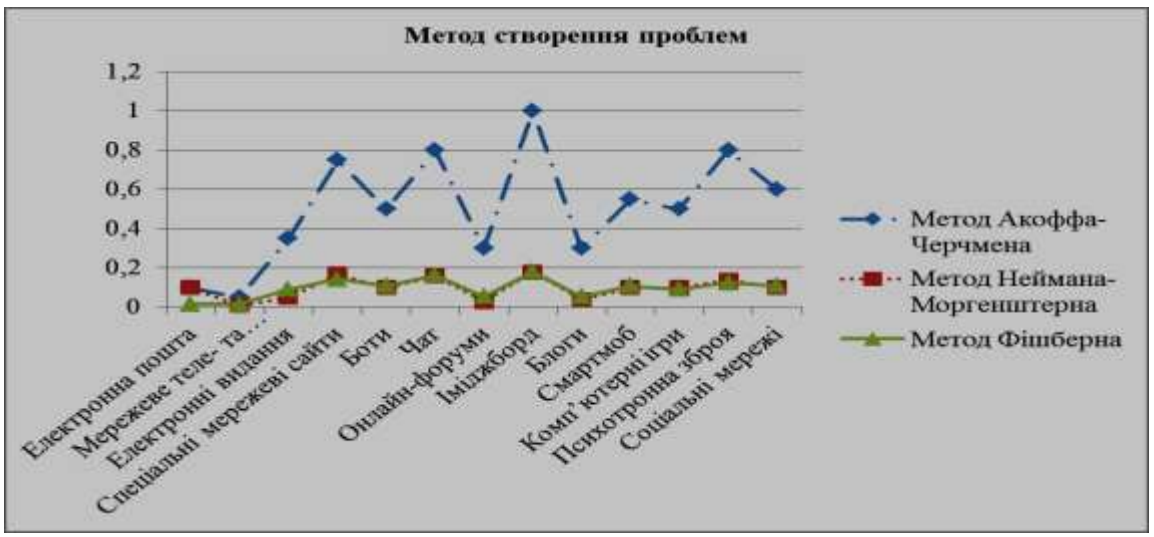

Рис. 7. Оцінки пріоритетів для методу “створення проблем”.

Метод “закидання брудом”. Політичне маніпулювання – приховане управління політичною свідомістю та поведінкою людей з метою примусити їх діяти (або лишатися бездіяльними) всупереч особистим інтересам [7; 13; 15]. Як зазначалося, метод “закидання брудом” полягає в підборі таких епітетів і такої лексики, що дають предмету розмови жорстко негативну етичну оцінку. Цей метод зараховується до числа найгрубіших пропагандистських прийомів, проте частіше від інших використовується в сучасній політично-інформаційній боротьбі. За допомогою цього методу образ “клієнта” перетворюється на суцільне “втілення зла” і під таким соусом визріває в масовій свідомості. Метод “закидання брудом” найбільш ефективний для таких Інтернет-ресурсів, як: *електронні видання, онлайн-форуми, блоги, мережеве теле- та радіомовлення, комп’ютерні ігри* (оцінку пріоритетів див. Рис. 8).

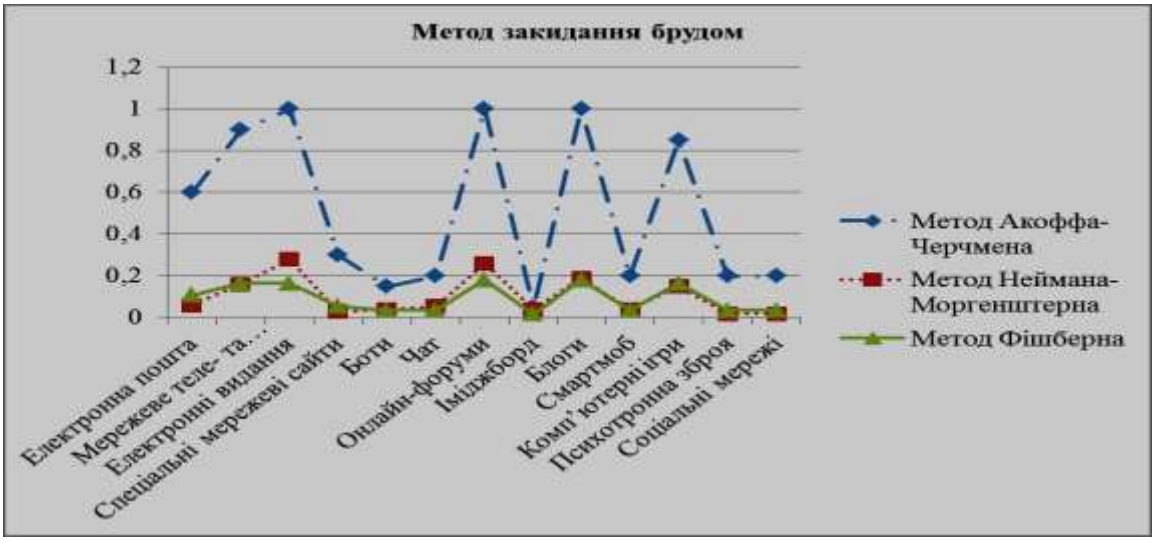

Рис. 8. Оцінки пріоритетів для методу “закидання брудом”.

Метод “відволікання уваги”. Застосовується для того, щоб відвернути увагу аудиторії від важливої, але невигідної маніпуляторам інформації за допомогою подання іншої інформації в максимально сенсаційній формі. Так, до прикладу, для відволікання уваги російської громадськості від злочинів РФ на території Донбасу, анексії Криму та усвідомлення масштабів наслідків, з якими росіянам доведеться зіткнутися, глава

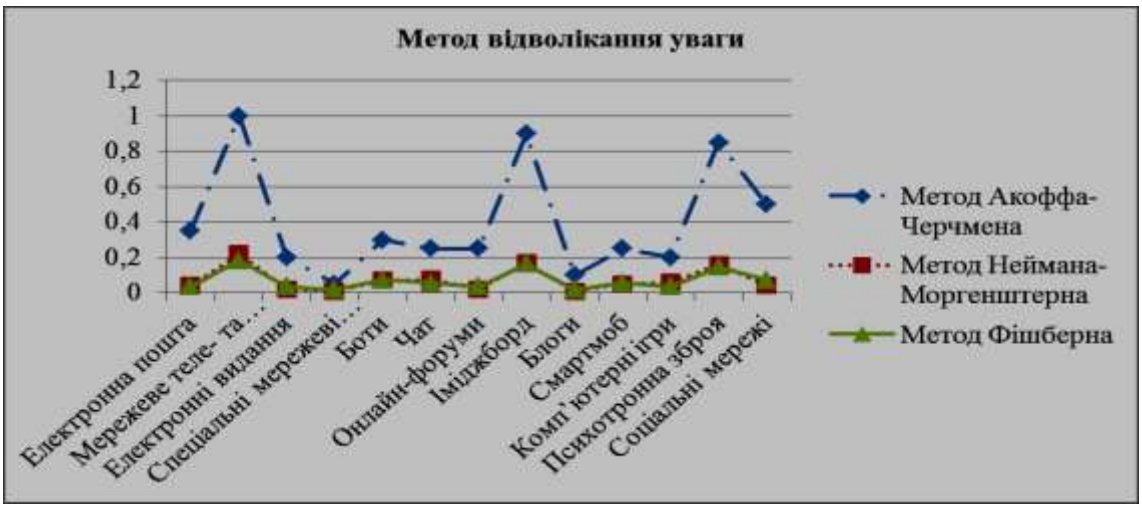

Рис. 9. Оцінки пріоритетів для методу “відволікання уваги”.

Слідчого комітету РФ Олександр Бастрикін своєю сенсаційною заявою про те, що Прем’єр-міністр України Арсеній Яценюк “воював” у 1990-х в Чечні, скористався цим улюбленим методом кремлівських пропагандистів, створивши у такий спосіб відволікаючу емоційну домінанту у російському суспільстві.

Згідно з розрахунками, метод відволікання уваги найбільш ефективний для таких Інтернет-ресурсів, як: *мережеве теле- та радіомовлення, іміджборд, психотронна зброя*. Це підтверджує той факт, що нині мас-медіа, в тому числі й електронні, є провідним чинником політичної соціалізації мас, що формують громадську думку щодо найважливіших політичних проблем (оцінку пріоритетів див. Рис. 9).

Метод “історичних аналогій”. Грецьким словом “аналогія” позначається подібність предметів та явищ в будь-яких властивостях. Широке використання методу “історичних аналогій” для маніпулювання свідомістю випливає з універсальних фундаментальних принципів буття. Як зазначають фахівці, метод “історичних аналогій” вельми вигідний у багатьох аспектах. По-перше, пропагандист отримує змогу підлеститися до аудиторії, апелюючи до її ерудованості. По-друге, в історії й справді можна підібрати приклади чи не на всі випадки життя. Цей метод до того ж допомагає в конструюванні “історичних” метафор, котрі програмують об’єкт впливу, а також і потрібних “історичних міфів”, що використовуються в стратегічній перспективі [5; 7; 15].

Нині метод “історичних аналогій” найбільш ефективний для таких Інтернет-ресурсів, як: *комп'ютерні ігри* (оцінку пріоритетів див. Рис. 10).

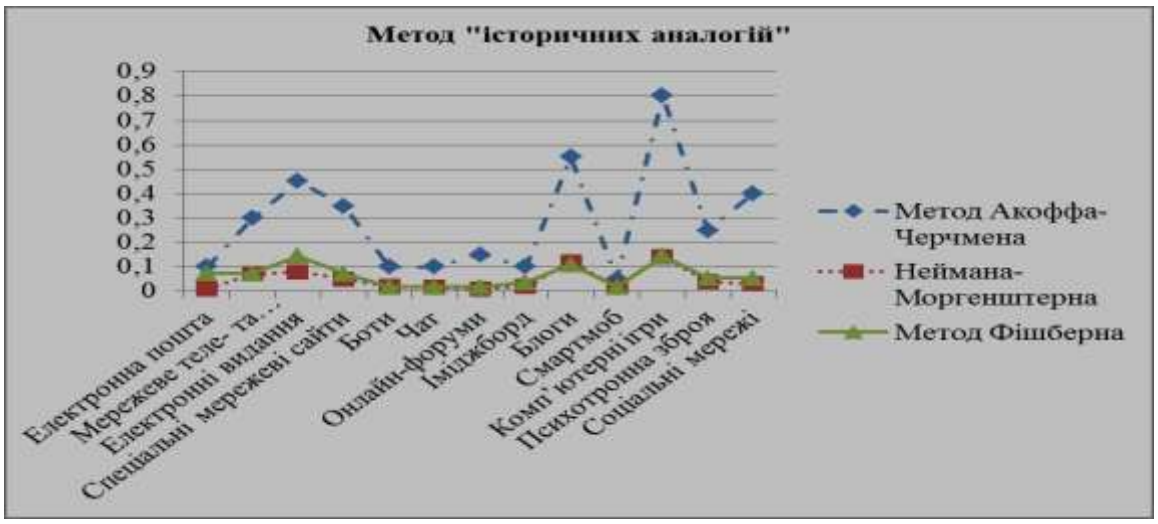

Рис. 10. Оцінки пріоритетів для методу “історичних аналогій”.

Розуміння сутності, способів використання методу аналогій є важливим фактором протидії сугестивним впливам.

Висновки.

Сучасний розвиток науки й техніки набув такого масштабу, коли створена реальна можливість масового поширення новітніх технологій, що дають змогу застосовувати засоби прямого й опосередкованого впливу на нервову систему та психіку для деструктивного впливу на великі групи людей. Унаслідок чого постала значна соціальна загроза застосування Інтернет-технологій для штучної зміни поведінкової реакції людини, її психічного стану і здоров’я, включаючи штучне вироблення психічної залежності. Як показали дослідження серед сучасних методів маніпуляції свідомістю найбільш актуальними є наступні: метод “ствердження”, метод “дезінформація”, метод “фокусу на емоції”, метод “використання стереотипів”, метод “повтору інформації”,

метод “міфів”, метод “створення проблем”, метод “закидання брудом”, метод “відволікання уваги”, метод “історичних аналогій”.

Сугестія може бути змодельована й одночасно досліджена в рамках багатьох наукових дисциплін, що вкрай ускладнює її дослідження. Першим кроком для побудови її математичної моделі можна розглядати системну процедуру ранжування як спосіб оцінки об’єктів у порядковій шкалі, коли кожному з них приписується місце в послідовності об’єктів. Через такий характер сугестії з типом шкали тісно пов’язані способи обробки і представлення результатів вимірювань. Адекватними методами, що стосуються оцінки пріоритетності негативного впливу на свідомість людини, можуть слугувати методи Акоффа-Черчмена, Неймана-Моргенштерна та метод Фішберна.

Розглянуті методи експертних оцінок мають різні якості, але призводять у загальному випадку до близьких результатів. Практика застосування цих методів показала, що найбільш ефективне їх комплексне застосування для вирішення однієї і тієї самої проблеми. Порівняльний аналіз результатів підвищує обґрунтованість сформульованих висновків. При цьому слід враховувати, що методом, який вимагає мінімальних витрат, є метод Фішберна, а найбільш трудомістким – метод послідовного порівняння (Черчмена – Акоффа).

Доцільність використання цих методів зумовлена також тим, що коефіцієнти пріоритетності сугестивного впливу можна використовувати для визначення загального показника інформаційно-психологічної безпеки людини, пов’язаного з кожною окремою інтернет-технологією маніпулювання.

Використана література

1. Бешелев С.Д. Математико-статистические методы экспертных оценок / С.Д. Бешелев, Гурвич Ф.М. – М. : Статистика, 1980. – 263 с.

2. Вдовин В.М. Теория систем и системный анализ / В.М. Вдовин, Л.Е. Суркова, В.А. Валентинов. – М. : ИТК “Дашков и К^{0}”, 2014. – 644 с.

3. Волкова В.Н. Теория систем : учебное пособие / В.Н. Волкова, А.А. Денисов. – М. : “Высшая школа”, 2006. – 511с.

4. Гнатієнко Г.М. Експертні технології прийняття рішень / Г.М. Гнатієнко, В.Є. Снитюк. – К. : ТОВ “Маклаут”, 2008, - 444 с.

5. Доценко Е.Л. Психология манипуляции: феномены, механизмы и защита / Е.Л. Доценко. – СПб. : Речь, 2003. 304 с.

6. Інформаційна безпека (соціально-правові аспекти) : підруч. / [В.В. Остроухов, В.М. Петрик, А.А. Штоквиш та ін.] ; за заг. ред. Є.Д. Скулиша. – К. : КНТ, 2010. – 776 с.

7. Кара-Мурза С.Г. Манипуляция сознанием / С.Г. Кара-Мурза. – М. : Алгоритм, 2004. – 528 с.

8. Куалман Э. Безопасная Сеть. Правила сохранения репутации в эпоху социальных медиа и тотальной публичности / Э. Куалман. – М. : Альпина Паблишер, 2017. – 214 с.

9. Качинська К.А. Інформаційно-психологічна безпека : система підтримки прийняття рішень в умовах сугестивного ризику : зб. наукових праць. XIV Міжнародна науково-практична конференція [“Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях”], (Київ, 5 – 9 жовтня 2015 р.). – К., 2015.

10. Качинська К.А. Інтернет-технології маніпулювання свідомістю особи, суспільства та держави : зб. наукових праць. XV Міжнародна науково-практична конференція [«Сучасні інформаційні технології управління екологічною безпекою, природокористуванням, заходами в надзвичайних ситуаціях»], (Київ, 3 – 6 жовтня 2016 р.). – К., 2016.

11. Литвак Б.Г. Экспертная информация : методы получения и анализа / Б.Г. Литвак. – М. : Радио и связь, 1982. – 184 с.

12. Миркин Б.Г. Анализ качественных признаков : математические модели и методы / Б.Г. Миркин. – М. : Статистика, 1976. – 166 с.

13. Морозов Е. Интернет как иллюзия. Обратная сторона сети / Е. Морозов. – М : Изд-во АСТ, 2014 . – 528 с.

14. Перегудов Ф.И. Введение в системный анализ / Ф.И. Перегудов, Ф.П. Тарасенко. – М. : Высшая школа, 1989, 367 с.

15. Почепцов Г. Информационные войны. Новый инструмент политики / Г. Почепцов. – М. : Алгоритм, 2015. – 256 с.

16. Сугестивні технології маніпулятивного впливу : навч.посіб / [В.М. Петрик, М.М. Присяжнюк, Л.Ф. Компанцева, Є.Д. Скулиш. О.Д. Бойко. В.В. Остроухов] ; за заг. ред. Є.Д. Скулиша. – К. : Наук. вид. НА СБ України, 2010. – 248 с.

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

Інформаційна і національна безпека

УДК 342.4:327.7

ТКАЧУК Т.Ю., *кандидат юридичних наук, доцент*, заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки Національної академії СБ України

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ОКРЕМИХ КРАЇН СХІДНОЇ ЄВРОПИ

Анотація. *Стаття присвячена дослідженню питань забезпечення інформаційної безпеки у країнах Східної Європи. В ході дослідження визначаються пріоритети та проблеми забезпечення інформаційної безпеки у вказаних країнах. Також оцінюється значущість досвіду країн Східної Європи у сфері забезпечення інформаційної безпеки для України.*

Ключові слова: *інформаційна безпека, безпека інформації, персональні дані, кібербезпека, Східна Європа.*

Summary. *The article is devoted to the research of the information security subject in the countries of Eastern Europe. The study identifies priorities and problems of ensuring information security in these countries. The importance of the experience of Eastern European countries in the field of information security for Ukraine is also assessed.*

Keywords: *information security, the defense of information, personal data, cybersecurity, Eastern Europe.*

Аннотация. *Статья посвящена исследованию вопросов обеспечения информационной безопасности в странах Восточной Европы. В ходе исследования определяются приоритеты и проблемы обеспечения информационной безопасности в указанных странах. Также оценивается значимость опыта стран Восточной Европы в сфере обеспечения информационной безопасности для Украины.*

Ключевые слова: *информационная безопасность, безопасность информации, персональные данные, кибербезопасность, Восточная Европа.*

Постановка проблеми. Підходи до забезпечення інформаційної безпеки, прийняті у країнах Східної Європи, наразі не є уніфікованими, що зумовлено геополітичною специфікою відповідних країн, одні з яких входять до Північноатлантичного Альянсу (НАТО) та Європейського Союзу (ЄС), інші – прямують до членства у вказаних організаціях, а деякі – входять до євразійських міждержавних утворень. Обравши євроінтеграційний курс та визначивши вступ до НАТО своїм стратегічним пріоритетом, Україна має орієнтуватися передусім на стратегію розвитку країн-учасниць ЄС та НАТО в інформаційній сфері [1, с. 18]. Втім, не менш важливим є і досвід інших країн Східної Європи, які проходять аналогічний шлях у процесі становлення та розвитку інформаційного суспільства. Тож дослідження, оцінка та імплементація позитивного досвіду східноєвропейських країн мають важливе значення при розбудові системи забезпечення інформаційної безпеки в Україні, оскільки події останніх років в нашій державі показали, що наша країна поки що не готова протистояти інформаційним війнам, а її політика у сфері забезпечення інформаційної безпеки та інформаційна політика в цілому потребує вдосконалення [2, с. 179].

Результати аналізу наукових публікацій. Проблематику інформаційної безпеки у країнах Європи, в тому числі – у східноєвропейських, досліджували у своїх роботах О. Запорожець, О. Климчук, С. Лазовський, Р. Лук’янчук, О. Павловська, В. Петров, А. Руснак. Дослідженням інформаційної безпеки України у контексті світового досвіду займалися І. Беззуб, О. Довгань, В. Глуховеря, Л. Задорожня, В. Кирик, О. Костенко, В. Ліпкан, А. Марущак, Е. Макаренко, В. Політанський, В. Роговець та інші науковці. Однак питання забезпечення інформаційної безпеки в країнах Східної Європи та доцільності використання їх досвіду для України поки що недостатньо висвітлені у науковій літературі.

Метою статті є дослідження питань забезпечення інформаційної безпеки у країнах Східної Європи, а також оцінка значущості для України досвіду країн Східної Європи у цій сфері.

Виклад основного матеріалу. З точки зору забезпечення інформаційної безпеки у Східній Європі доцільно буде визначити репрезентативними країни різних геостратегічних спрямувань, тому в рамках цієї статті пропонуємо зосередитись на огляді питань забезпечення інформаційної безпеки у Румунії, Болгарії, Молдові та Білорусі.

Передусім зауважимо, що Румунія та Болгарія є членами Північноатлантичного Альянсу та Європейського Союзу. Відповідно, на них поширюються стандарти цих міжнародних організацій щодо інформаційної політики та забезпечення інформаційної безпеки. Це, зокрема, стандарти НАТО щодо захисту інформації, викладені у Документі СМ (2002)49 “Безпека в організації Північноатлантичного договору (НАТО)” [3], офіційна політика НАТО у сфері кіберзахисту [4 – 5], стратегічна концепція кібербезпеки, сформульована за результатами Лісабонського саміту [6] й уточнена за результатами Варшавського саміту [7] тощо. Також Румунія та Болгарія, як країни-члени ЄС, втілюють у національній політиці забезпечення інформаційної безпеки стандарти ЄС, в тому числі передбачені “Європейськими критеріями безпеки інформаційних технологій” (1991 р.) [8], “Єдиними критеріями безпеки інформаційних технологій” (1996 р.) [9], документом “Мережева та інформаційна безпека: європейський політичний підхід” (2001 р.) [10], документом “На шляху до загальної політики в сфері боротьби з кіберзлочинністю” (2007 р.) [11] тощо. Відповідно, основними напрямами забезпечення інформаційної безпеки у вказаних країнах є: підвищення обізнаності користувачів щодо можливих загроз під час користування комунікаційними мережами; створення європейської системи попередження та інформування про нові загрози; забезпечення технологічної підтримки; підтримка ринково орієнтованої стандартизації та сертифікації; правове забезпечення, пріоритетами якого є захист персональних даних, регламентація телекомунікаційних послуг та протидія кіберзлочинності; зміцнення інформаційної безпеки на державному рівні шляхом впровадження ефективних і сумісних засобів забезпечення інформаційної безпеки та заохочення використання країнами-членами електронних підписів під час надання державних он-лайн послуг тощо; розвиток міжнародного співробітництва з питань інформаційної безпеки. Основними викликами інформаційній безпеці Румунії та Болгарії, як країн ЄС, є некоординовані національні підходи до безпеки інформаційних інфраструктур, що знижує ефективність національних заходів; відсутність на європейському рівні партнерства між державним та приватним секторами; обмежені можливості щодо раннього попередження та реагування на безпекові інциденти, зумовлені нерівномірністю розвитку систем моніторингу і сповіщення про інциденти у країнах-членах, нерозвиненістю міждержавного співробітництва та обміну інформацією щодо цих проблем; відсутність міжнародного консенсусу щодо пріоритетів у реалізації політики захисту критичної інформаційної інфраструктури [12].

Одним з найбільш важливих питань політики інформаційної безпеки Румунії та Болгарії, як країн-членів ЄС, є захист персональних даних, в якому вони керуються положеннями Директиви 95/46/ЄС “Про захист фізичних осіб у зв’язку з обробкою персональних даних і вільного обігу таких даних”. У цьому документі одночасно декларується прагнення до вільного переміщення інформації між країнами-членами ЄС та надаються гарантії захисту основних прав громадян, до яких входить право на недоторканність особистих даних і їх захист від третіх осіб [13 – 14]. Крім того, з 2018 року для Румунії та Болгарії, як і інших країн-членів ЄС, набудуть чинності нові правила захисту персональних даних (GDPR), які схвалено 14 квітня 2016 року. Ці правила буде поширено не тільки на європейські компанії, але й на компанії з інших країн, які пропонують товари й послуги в ЄС. У відповідному документі переглянуті цивільні права користувачів, відповідальність за схоронність даних, а також уведені деякі обмеження переміщення даних між різними країнами. Також важливим нововведенням є введення більш суворого покарання за несвоєчасне повідомлення інформації про виток даних. Компаніям, що порушили положення нової директиви та не доповіли про факт витоку або злому протягом 72 годин з моменту виявлення інциденту, загрожує штраф до 4 % річного доходу або до 20 млн. євро [15]. Крім того, відповідна Директива передбачає необхідність отримання згоди користувачів на обробку їх персональних даних, причому на обробку даних з різними цілями потрібні будуть окремі згоди. Згода повинна бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Згода не буде вважатися вільною, якщо користувач змушений дати таку згоду, щоб одержати доступ до сайту, програми або додатка. Виключенням є випадки, коли персональні дані користувача потрібні для виконання угоди. У випадках, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних. Компанії, що працюють із персональними даними, також повинні будуть вести облік операцій з персональними даними (тип даних і цілі, для яких вони обробляються), мінімізувати використання персональних даних відповідно до принципу data protection by design, а також проводити внутрішній аудит [16].

Не менш гостро, ніж проблема захисту персональних даних, у Румунії та Болгарії усвідомлюється небезпечність загроз, що виходять з кіберпростору.

Так, у Румунії на сьогоднішній день активно триває процес розбудови системи кібернетичної безпеки держави як на законодавчому, так і на організаційному рівнях. При цьому ключова роль у забезпеченні кібербезпеки Румунії відводиться її спеціальному контррозвідувальному органу – Румунській службі інформації, у структурі якої створено національний центр кібербезпеки [17, с. 79-80]. Головною функцією цього центру є поєднання систем технічного захисту із можливостями спецслужби з метою отримання інформації, необхідної для попередження, припинення та подолання наслідків кібератак на інформаційно-телекомунікаційні системи об’єктів критичної інфраструктури держави [18]. Законопроект “Про кібербезпеку”, який у грудні 2014 року був схвалений сенатом Румунії, також передбачає створення Національної системи кібернетичної безпеки Румунії, технічну координацію якої покладено на Румунську службу інформації як головного суб’єкта кібербезпеки держави [19].

Національна стратегія забезпечення кібербезпеки Румунії (2013 р.) при цьому передбачає, що Румунія забезпечує функціонування динамічного інформаційного середовища на основі функціональної сумісності й послуг, характерних для інформаційного суспільства, а також забезпечення відповідності основних прав і свобод громадян та інтересів національної безпеки у відповідних правових рамках. Важливим

для цього є розвиток культури кібербезпеки користувачів комп’ютерів і телекомунікаційних систем, їх поінформованість щодо потенційних ризиків, а також про можливості їх мінімізації. Збільшення поінформованості щодо ризиків і загроз, пов’язаних з діяльністю, здійснюваною в кіберпросторі, а також способів запобігання та протидії їм вимагають ефективної комунікації й співробітництва між всіма учасниками діяльності у цій сфері, тож Румунська держава бере на себе роль координатора заходів, здійснюваних на національному рівні, забезпечуючи кібербезпеку відповідно до визначених під керівництвом ЄС і НАТО підходів.

З метою забезпечення кібербезпеки Румунії Стратегія визначає наступні цілі: адаптація нормативного й інституціонального підґрунтя до динаміки конкретних загроз у кіберпросторі; встановлення й застосування мінімальних профілів і вимог безпеки для національних кіберсистем, що забезпечують правильну роботу критичної інфраструктури; забезпечення стійкості кіберінфраструктури; забезпечення безпеки шляхом усвідомлення й запобігання уразливостям та ризикам, а також протидії загрозам кібербезпеці Румунії; використання можливостей кіберпростору для просування інтересів, цінностей та національних цілей в кіберпросторі; сприяння та розвиток співробітництва між державним і приватним секторами на національному рівні, а також міжнародне співробітництво у сфері кібербезпеки; розвиток культури безпеки населення шляхом усвідомлення уразливостей, ризиків і загроз з кіберпростору та необхідності захисту власних інформаційних систем; активна участь в ініціативах міжнародних організацій, учасницею яких є Румунія, в рамках реалізації комплексу заходів щодо зміцнення довіри до міжнародного використання кіберпростору. Особливу увагу Стратегія приділяє розвитку національних можливостей щодо управління ризиками у сфері кібернетичної безпеки [20].

На думку Консультативної ради з питань національної безпеки Болгарії, кібербезпека і стабільність мають стратегічне значення для розвитку електронного урядування в Болгарії й досягнення оперативної сумісності в роботі адміністрації в цифровому середовищі шляхом введення загальних стандартів. Відповідно, необхідно прискорене впровадження комплексу заходів щодо забезпечення безпеки електронної ідентичності громадян, а також щодо забезпечення захищеної й оптимізованої сумісності електронної ідентичності з такими компонентами, як електронний підпис. Тож у квітні 2016 року Консультативна рада представила Парламенту Болгарії проект Національної стратегії кібербезпеки під назвою “Стійка до кібератак Болгарія 2020”, яка передбачає реалізацію наступних заходів: ініціювання законодавчих змін з метою остаточного прийняття й транспонування Директиви ЄС і Європейського Парламенту про заходи щодо забезпечення високого загального рівня мережної й інформаційної безпеки в ЄС, а також для захисту політичних і виборчих прав громадян і в кіберпросторі; забезпечення цільових ресурсів, необхідних для створення належного потенціалу для кібербезпеки та удосконалення ІТ-інфраструктури, а також реалізації мережної моделі обміну інформацією й координації між організаціями, відповідальними за кібербезпеку у Болгарії; забезпечення Міністерства внутрішніх справ, Агентства національної безпеки, Міністерства оборони, Міністерства транспорту й Державного агентства розвідки необхідними фінансовими ресурсами з поступовим збільшенням числа експертів з питань кібербезпеки для запобігання й боротьби з кіберзагрозами; організація й проведення національних навчань з кіберстійкості з тестуванням ключових елементів Національної стратегії кібербезпеки й ефективності чинних контрзаходів; зміцнення співробітництва з ЄС і НАТО щодо забезпечення кібербезпеки; покладання на державні установи обов’язку щодо вчасного інформування компетентних служб

щодо фактів здійснених на них кібератак. Національна стратегія була прийнята Радою міністрів Республіки Болгарії 13 липня 2016 року.

Відповідно до п. 4.7.1 Національної стратегії, провідну роль у забезпеченні кіберзахисту країни відіграє Міністерство оборони Болгарії. Ефективне забезпечення кібербезпеки при цьому передбачає розбудову існуючих та створення нових розширених можливостей для кіберзахисту, сумісних з вимогами НАТО і ЄС, а також проведення адекватних структурних і організаційних реформ, зокрема: розробку політики у сфері забезпечення кібербезпеки, розробку відповідної концепції й методичних документів, що передбачають захист національної безпеки шляхом активної протидії кібер- і гібридним загрозам у кіберпросторі; реалізацію інвестиційних проектів для кіберзахисту у рамках спільних ініціатив, у тому числі ініціативи НАТО/ЄС “Smart Defense” та “об’єднання й спільного використання”, а також створення можливостей для кібероборони в рамках загального процесу планування у сфері оборони; створення Оперативного центру кіберзахисту відповідно до плану розвитку Збройних сил Болгарії до 2020 року за допомогою центру NCIRC НАТО із забезпеченням безперервного моніторингу і повної оперативної інтеграції в національну мережу NKOMKS, розвиток колективного потенціалу реагування на кібер- і гібридні загрози на національному й міжнародному рівні; погоджений обмін інформацією про кіберінциденти за допомогою державних установ, НАТО і ЄС, а також співробітництво з діловими й науковими колами; накопичення досвіду у сфері кіберзахисту й підвищення професійної підготовки персоналу шляхом періодичної підготовки й участі в навчаннях, розширення участі у роботі центру кіберзахисту НАТО та інших партнерських центрів; удосконалювання й розвиток взаємодії із промисловістю й науково-дослідними організаціями на основі “кластерної кібероборони”; активну участь у міжнародних програмах НАТО і ЄС у рамках науково-дослідних проектів; адаптація й впровадження моделі ES75 щодо спільного використання ресурсів на національному рівні для професіоналів, інші форми залучення експертів з кіберпромисловості та наукових кіл. Пункт 7.3 Стратегії передбачає створення механізмів і технічних ресурсів для постійного моніторингу можливих загроз кібербезпеці з точки зору масштабів, джерел і природи (кібер-, гібридні), тенденцій у геополітичному контексті й аналізу національної картини кібербезпеки, а також розвитку здатності застосовувати адекватні форми протидії, в т.ч. підтримувати створення джерел контр-інформаційних впливів [21].

Незважаючи на критику політики забезпечення інформаційної безпеки у наукових колах [22, с. 63], у Молдові діє відносно надійна система протидії кіберзлочинності. Так, ще у 2009 році Парламентом була ратифікована Конвенція Ради Європи про кіберзлочинність [23]. Крім того, влада Молдови підписала Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах у березні 2012 року [24]. Парламентом також був прийнятий Закон “Про попередження та боротьбу зі злочинністю у сфері комп’ютерної інформації” у січні 2010 року [25]. Згідно із цим Законом генпрокуратура Молдови наділена повноваженнями координувати й здійснювати кримінальне переслідування осіб, що вчинили кіберзлочини. Метою Закону є вдосконалення регламентації правовідносин за такими напрямками: запобігання та боротьба з кіберзлочинністю, сприяння провайдерам і користувачам інформаційних систем, співробітництво державних служб із неурядовими організаціями та іншими представниками громадянського суспільства, а також міжнародне співробітництво з організаціями й країнами, що мають досвід у відповідних питаннях. Генеральною прокуратурою з метою сприяння розслідуванням був відкритий Центр розслідування

кіберзлочинів, один з відділів якого уповноважений реагувати на випадки загроз безпеці в урядових структурах, бізнесі й громадському секторі.

Також у Молдові здійснено низку інших заходів щодо зміцнення інформаційної безпеки. Так, у результаті ратифікації Факультативного протоколу до Конвенції ООН про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії [26], Конвенції Ради Європи про кіберзлочинність [23] й Конвенції Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства [27], Молдова стала активним учасником процесу застосування загальної кримінальної політики у сфері боротьби з інформаційною злочинністю, у тому числі злочинами, пов’язаними із онлайн-експлуатацією дітей.

Важливим кроком на національному рівні стало також затвердження Закону Молдови “Про електронний підпис та електронний документ” від 29 травня 2014 року, розробленого з метою підвищення рівня безпеки електронних підписів та приведення у відповідність із міжнародними стандартами й рекомендаціями щодо інфраструктури відкритих ключів [28]. В цілому слід зауважити, що у Молдові розпочато процес приведення чинного законодавства у відповідність до положень Директиви 2006/24/ЄС “Про зберігання інформації, створеної або обробленої при наданні послуг зв’язку загального користування або мереж зв’язку загального користування й внесення змін у Директиву ЄС 2002/58/ЄС” від 15 березня 2006 року щодо захисту персональних даних [29], Директиву 2008/114/ЄС “Про ідентифікацію й призначення європейських критичних інфраструктур і заходах з їх захисту” від 8 грудня 2008 року [30] тощо.

З метою забезпечення системного підходу й формування державної політики у сфері забезпечення інформаційної безпеки, яка об’єднала б правові, організаційні, технічні, технологічні й фізичні заходи щодо захисту кіберпростору Молдови, а також чіткої регламентації функцій і повноважень підвідомчих структур, Уряд Республіки Молдова Постановою від 31 жовтня 2013 року № 857 затвердив Національну стратегію розвитку інформаційного суспільства “Moldova digitală 2020” (Цифрова Молдова 2020) і План дій з її впровадження, розроблений Міністерством інформаційних технологій та зв’язку [31]. У Стратегії вперше розглядається проблема створення умов для підвищення ступеня безпеки й довіри до кіберпростору, а ключові дії щодо створення цих умов становлять окрему главу вищезгаданого Плану дій. Стратегія визначає, що використання нових технологій породжує численні можливості розвитку, але й численні ризики й уразливості, що вимагають підвищеної уваги держави й зацікавлених учасників. Ці ризики характеризуються асиметрією, вираженою динамікою й глобальним характером, що ускладнює їхнє виявлення й протидію за допомогою заходів, пропорційних до ефекту їхньої матеріалізації. То ж попередження і боротьба з кібератаками, у тому числі зі злочинністю в цій сфері є одним із пріоритетів міжнародних організацій, а їх бурхливий ріст на світовому рівні на 600 % з 2005 року вказує на нагальну необхідність вжиття заходів щодо страхування інформаційної інфраструктури Республіки Молдова від можливих ризиків, пов’язаних з незаконною діяльністю у цій сфері. Важливість цієї проблеми була відзначена у Концепції національної безпеки й Стратегії національної безпеки Республіки Молдова, у яких були встановлені цілі системи забезпечення національної безпеки та загрози у інформаційній сфері [32].

Проект Концепції інформаційної безпеки, схвалений Парламентом Молдови в першому читанні 23 червня 2017 року, викликав у суспільстві неоднозначну реакцію. На думку експертів, останні ініціативи щодо регламентації інформаційного простору містять цілу низку серйозних прогалин, які можуть призвести до зловживань. Зокрема, Концепцію інформаційної безпеки доцільно узгодити із новою Стратегією національної

безпеки, однак останній проект Стратегії національної безпеки в червні 2017 року був відкликаний з Парламенту Президентом, а новий проект досі не розроблений. Крім того, проект Концепції припускає занадто суворий контроль Інтернету з боку деяких держустанов, зокрема Служби інформації та безпеки Республіки Молдова, які зможуть втручатися в діяльність провайдерів, а також контролювати інформаційний простір, включаючи соціальні мережі. Однак, з урахуванням того, що населення дедалі активнвше користується Інтернетом, і на цьому тлі влада починає втрачати контроль над інформацією, це не єдина законодавча ініціатива у сфері інформаційної безпеки, захисту інформації, протистояння кіберзлочинності й боротьби зі зловживаннями в Інтернеті – серед таких ініціатив слід згадати, зокрема, законопроект № 161, більш відомий як “Великий брат”, і законопроект № 281, що одержав назву “Мандат безпеки”, який уточнює правила проведення спеціальних розшукових заходів в інформаційному просторі й припускає розширення повноважень спеціальних служб у цій сфері. За оцінками фахівців, спроби держави встановити контроль над інформаційними мережами у спосіб, який передбачається цими законопроектами, не стільки забезпечать ефект безпеки інформаційного простору, скільки вдарить по громадянському суспільству, політичних партіях, простих громадянах, яким обмежать можливості висловлювати свою думку й критичні зауваження на адресу влади [33].

У Білорусі нагляд за інформаційним простором та система обмежень наразі є ключовими елементами державної політики забезпечення інформаційної безпеки, зокрема, державні органи відстежують протестні настрої за допомогою складного російського устаткування для моніторингу, впровадженого телекомунікаційними компаніями. З 2010 до 2015 року у країні діяла Постанова Оперативно-аналітичного центру при Президентові Республіки Білорусь і Міністерства зв’язку та інформатизації Республіки Білорусь “Про затвердження Положення про порядок обмеження доступу користувачів Інтернет-послуг до інформації, забороненої до поширення відповідно законодавчих актів” від 29.06.10 р. № 4/11, за змістом якої провайдери мали фільтрувати Інтернет-контент відповідно до двох чорних списків url-адрес, один з яких перебував у публічному доступі, а інший – був доступний тільки провайдерам (закритий список містив приблизно 80 url-адрес, доступ до яких було обмежено у державних, культурних і урядових закладах, і включав популярні опозиційні сайти на кшталт Charter97.org і Belaruspartisan.org) [34]. Наразі ж відповідні обмеження реалізуються відповідно до Указу Президента Республіки Білорусь “Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет” від 01.02.10 р. № 60, Декрету Президента Республіки Білорусь “Про невідкладні заходи з протидії незаконному обігу наркотиків” від 28.12.14 р. та Закону Республіки Білорусь “Про засоби масової інформації” від 17.07.08 р. [35].

У березні 2010 року від білоруських провайдерів зажадали більш тісного співробітництва з державними системами спостереження (СОРМ), які здійснює повний он-лайн-нагляд у всій країні, що регламентується значною кількістю нормативно-правових актів. Як і в Росії та сусідніх країнах, СОРМ Білорусі дає виконавчим органам і органам національної безпеки можливість здійснювати перехоплення повідомлень з будь-яких комунікаційних каналів з метою боротьби зі злочинністю. Провайдери Інтернет-послуг і оператори зв’язку зобов’язані встановлювати відповідне устаткування й надавати державним органам цілодобовий доступ до нього. Відповідно до Указу Президента Республики Беларусь “Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет” від 01.02.10 р. № 60 [36], провайдери повинні вести облік IP-адрес, а держава може витребувати інформацію щодо Інтернет-діяльності будь-якого громадянина. З 2007 року до Інтернет-кафе пред’являється вимога зберігати

історію Інтернет-активності користувачів протягом одного року й інформувати виконавчі органі про підозрілі дії [34]. СОРМ працює, головним чином, відповідно до Закону “Про оперативно-розшукову діяльність” [37], Закону “Про органи державної безпеки Республіки Білорусь” [38] та Указу “Про затвердження Положення про порядок взаємодії операторів електрозв’язку з органами, що здійснюють оперативно-розшукову діяльність” № 129 [39].

У Білорусі немає спеціальних законів, присвячених протидії кіберзлочинності, але деякі аспекти регулюються Кримінальним кодексом і законами, що стосуються регламентації діяльності глобальної інформаційної мережі Інтернет. Білорусь також подавала заявку на приєднання до Конвенції про кіберзлочинність, прийнятої в Будапешті в 2012 році [23], що й визначило необхідність дотримуватись відповідних міжнародних стандартів. Це був доволі неочікуваний для Білорусі крок, особливо у контексті тісних зв’язків з Росією, адже Китай і Росія виступили проти конвенції й висловилися на захист альтернативної концепції боротьби з кіберзлочинністю, у рамках якої держава одержувала значно більше повноважень, ніж це передбачалося Будапештською конвенцією.

За розслідування комп’ютерних злочинів у Білорусі відповідає спеціальне управління Міністерства внутрішніх справ, яке координує роботу з іншими виконавчими органами в Білорусі й аналогічними міжнародними організаціями в США, Євросоюзі, країнах СНД і в інших державах. У суспільстві висловлюються непоодинокі підозри, що це управління має справу здебільшого з переслідуванням порушників кримінального кодексу й не займається розробкою законодавства з питань кібербезпеки, а також бере участь у переслідуванні та он-лайн-відстеженні політичних активістів [34].

Що стосується участі Республіки Білорусь у забезпеченні кібербезпеки на регіональному рівні, слід зауважити, що Рада голів держав Співдружності Незалежних Держав (СНД) у 2013 році прийняла Концепцію співробітництва держав-членів СНД у боротьбі зі злочинами, що вчиняються з використанням інформаційних технологій [40]. Відповідно до цього документу країни-члени СНД обмінюються робочою, статистичною й методологічною інформацією та ведуть єдину базу даних щодо кіберзлочинців. На підставі цієї Концепції з 2015 року здійснюється розробка програми співробітництва між країнами СНД у боротьбі з кіберзлочинністю, яка підлягає затвердженню Радою Міністрів країн СНД. Також у 2017 році розпочато підписання нової Угоди про співробітництво держав-членів СНД у боротьбі зі злочинами у сфері інформаційних технологій [41].

Висновки.

Наразі країни Східної Європи вважають вирішення проблеми забезпечення інформаційної безпеки особи, суспільства, держави, їх захисту від внутрішніх та зовнішніх, у тому числі гібридних загроз, одним з найбільш важливих стратегічних пріоритетів забезпечення національної безпеки.

Україна має співпрацювати з іншими країнами Східної Європи у розбудові систем регіональної та міжнародної інформаційної безпеки з метою протидії загрозам стратегічній стабільності, таким, як кібертероризм та кіберзлочинність, орієнтуючись при цьому на стандарти ЄС та НАТО.

В цьому контексті для України є важливим досвід країн Східної Європи щодо приведення національного законодавства у відповідність до вимог вказаних міжнародних організацій, передусім – щодо забезпечення балансу між свободою й безпекою в інформаційній сфері на законодавчому рівні.

Використана література

1. Політанський В.С. Інформаційне суспільство в Україні : від зародження до сьогодення. // Науковий вісник Ужгородського національного університету. – (Серія “Право”). – Вип. 42. – 2017. – С. 16-22.

2. Шатун В.Т., Гладун О.В. Інформаційна безпека – невід’ємна складова національної безпеки України // Наукові праці. Державне управління. – Вип. 255. – Т. 267. – 2016. – С. 174-180.

3. Document C-V(2002)49 : Security within tne North Atlantic Treaty Organization (NATO) : [Online tool]. – Available at : http://www.statewatch.org/ news/2006/sep/nato-sec-classifications.pdf

4. NATO Bucharest Summit Declaration, 3 April 2008 : [Online tool]. – Available at : http://www.nato.int/docu/pr/2008/p08-049e.html

5. North Atlantic Treaty Organization. Active Engagement/ Modern Defence Strategic Concept For the Defence and Security of The Members of the North Atlantic Treaty Organisation : [Online tool]. – Available at : http://www.nato.int/ lisbon2010/strategic–concept–2010–eng.pdf

6. NATO Lisbon Summit Declaration, 20 Nowember 2010 : [Online tool]. – Available at : http://www.nato.int/docu/pr/2010/p10-049e.html

7. NATO Warsaw Summit Communiqué, 9 July 2016 : [Online tool]. – Available at : http://www.nato.int/cps/en/natohq/official_texts_133169.htm

8. Information Tecnhology Security Evaluation Criteria : [Online tool]. – Available at : https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf

9. Common Criteria for Information Technology Security Evaluation : [Online tool]. – Available at : https://www.commoncriteriaportal.org/files/ccfiles/CCPART 2V3.1R4.pdf

10. Communication from the European Commission: Network and Information Security: Proposal for a European Policy Approach. COM (2001) 298 : [Online tool]. – Available at : http://ec.europa.eu/information_society/eeurope/2002/ news_library/ pdf_files/netsec_en.pdf

11. Communication from the Commission : Towards a general policy on the fight against cyber crime. COM (2007) : [Online tool]. – Available at : http://eurlex.europa.eu/LexUriServ/site/en/com/ 2007/com2007_0267en01.pdf

12. Communication from the Commission on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM (2009)149 : [Online tool]. – Available at : http://ec.europa.eu/information_ society/policy/nis/strategy/activities/ ciip/index_en.htm

13. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 року. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_242

14. Nigel Waters, Graham. Interpreting the Security Principle : [Online tool]. – Available at : http://www.cyberlawcentre.org/ipp/wp/WP1%20Security.pdf

15. В Евросоюзе приняли новый закон о защите данных. – Режим доступу : https://threatpost.ru/v-evrosoyuze-prinyali-novyj-zakon-o-zashhite-dannyh/15749

16. Персональные данные : новые правила в Европейском Союзе. – Режим доступу : https://habrahabr.ru/post/300348

17. Климчук О.О., Ткачук Н.А. Роль і місце спецслужб та правоохоронних органів провідних країн світу в національних системах кібербезпеки // Інформаційна безпека людини, суспільства, держави. – 2015. – № 3 (19). – С. 75-83.

18. Cyberintelligence : [Online tool]. – Available at : https://www.sri.ro/cyberintelligence-en.html

19. The Senate passed the draft low regarding the cyber security of Romania : [Online tool]. – Available at: http://actmedia.ua/daily/the-senate-passed-the -draft-law-regarding-the ceber-security-of-romania/55734

20. Romania’s Cyber Security Strategy and the National Action Plan on Implementation of the National Cyber Security (2013) : [Online tool]. – Available at : https://www.cert.ro/vezi/document/ strategia-de-securitate-cibernetica

21. National Cyber Security Strategy : Cyber Resilient Bulgaria 2020 (2016) : [Online tool]. – Available at : https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Cybersecurity%20Forum%20Bulgaria/Bulgaria_sharkov_todorov.pdf

22. Руснак А.К. Молдова и информационная безопасность // SECURITATEA INFORMATIONALĂ 2011 : Conferinţa Internaţională, ediţia a VIII-a, 4 mai 2011. – P. 62-63.

23. Конвенція про кіберзлочинність від 23 листопада 2001 року. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/994_575

24. Другий додатковий Протокол до Європейської Конвенції про взаємну допомогу у кримінальних справах від 08 листопада 2001 року. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_518

25. Lege Nr. 20 din 03.02.2009 Privind prevenirea şi combaterea criminalităţii informatice : [Online tool]. – Available at : http://lex.justice.md/viewdoc.php?action=view&view=doc&id=333508&lang=1

26. Про права дитини, що стосується торгівлі дітьми, дитячої проституції й порнографії : Факультативний протокол до Конвенції ООН від 01 січня 2000 року. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/995_b09

27. Про захист дітей від сексуальної експлуатації та сексуального насильства : Конвенція Ради Європи від 25 жовтня 2007 року. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/ 994_927

28. Lege Nr. 91 din 29.05.2014 Privind semnătura electronică şi documentul electronic : [Online tool]. – Available at : http://lex.justice.md/viewdoc.php?action=view&view=doc&id=353612 &lang=1

29. Про збереження даних, створених або оброблених при наданні загальнодоступних послуг електронних повідомлень або громадських мереж зв’язку, та внесення поправок в Директиву 2002/58/ЄС : Директива 2006/24/ЄС Європейського парламенту та Ради Європи від 15 березня 2006 року. – Режим доступу : https://ain.ua/2009/10/27//директива-ес-о-сохранении-данных-укр

30. О европейских критических инфраструктурах и мерах по их защите : Директива 2008/114/ЕС Европейского парламента и Совета Європы от 08 декабря 2008 года. – Режим доступу : http://docs.pravo.ru/document/view/32671965/

31. HOTĂRÎRE Nr. 811 din 29.10.2015 Cu privire la Programul national de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 : [Online tool]. – Available at: http://lex.justice.md/viewdoc.php?action=view&view=doc&id= 361818&lang=1

32. Молдова : Национальный ИКТ-профайл. – (Информационная безопасность и защита информации). – Режим доступу : https://digital.report/moldova-informatsionnaya-bezopasnost

33. Мнения экспертов Молдовы : Законопроекты в области информационной безопасности противоречат друг другу, то есть ведут к злоупотреблениям. – Режим доступу : http://www.allmoldova.com/ru/project/mnenie/mnieniia-ekspiertov-moldovy-zakonoproiekty-v-oblasti-informatsionnoi-biezopasnosti-protivoriechat-drugh-drughu-to-iest-viedut-k-zloupotrieblieniiam

34. Беларусь : Национальный ИКТ-профайл. – (Информационная безопасность и защита информации). – Режим доступу : https://digital.report/belarus-informatsionnaya-bezopasnost

35. О признании утратившим силу постановления Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29 июня 2010 года № 4/11 : Постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 19 февраля 2015 года № 7/7. – Режим доступу : http://www.pravo.by/upload/docs/op/T21503058_1424811600.pdf

36. О мерах по совершенствованию использования национального сегмента сети Интернет : Указ Президента Республики Беларусь от 01 февраля 2010 года № 60. – Режим доступу : http://pravo.by/ document/?guid=3871&p0=P31000060

37. Об оперативно-розыскной деятельности : Закон Республики Беларусь от 15 июля 2015 года № 307-З. – Режим доступу : http://kgb.by/ru/zakon289-3

38. Об органах государственной безопасности Республики Беларусь : Закон Республики Беларусь от 10 июля 2012 года № 390-З. – Режим доступу : http://kgb.by/ru/zakon390-3

39. Об утверждении Положения о порядке взаимодействия операторов электросвязи с органами, осуществляющими оперативно-розыскную деятельность : Указ Президента Республики Беларусь от 03 марта 2010 года № 129. – Режим доступу : http://oac.gov.by/files/files/pravo/ukazi/Ukaz_129.htm

40. Концепция сотрудничества государств-участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий : утверждена Решением Совета глав государств СНГ от 25 октября 2013 года. – Режим доступу : http://www.e-cis.info/page.php?id=23808

41. Страны СНГ будут сотрудничать в борьбе с киберпреступностью. – Режим доступу : https://www.ritmeurasia.org/news--2017-08-28--strany-sng-budut-sotrudnichat-v-borbe-s-kiberprestupnostu-32043

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

УДК 342.591

КОПАН О.В., *доктор юридичних наук, професор,* головний науковий співробітник
НДІ інформатики і права НАПрН України

ДЕСТАБІЛІЗАЦІЯ СОЦІАЛЬНО-ПОЛІТИЧНОЇ СИТУАЦІЇ – ПРОВОКАЦІЯ ВНУТРІШНЬОДЕРЖАВНОГО КОНФЛІКТУ

Анотація. *У статті розкрито проблему навмисного створення умов для виникнення конфлікту, результатом якого є дестабілізація соціально-політичної ситуації в країні.*

Ключові слова: *внутрішньодержавний конфлікт, дестабілізація соціально-політичної ситуації, безпека, провокація, екстремізм, конфлікт безпеки.*

Summary*. The article deals with the problem of deliberate creation of conditions for the emergence of conflict, the result of which is the destabilization of the socio-political situation in the country.*

Keywords: *intra-state conflict, destabilization of socio-political situation, security, provocation, extremism, conflict of safety.*

Аннотация. *В статье раскрыта проблема умышленного создания условий для возникновения конфликта, результатом которого является дестабилизация социально-политической ситуации в стране.*

Ключевые слова: *внутригосударственный конфликт, дестабилизация социально-политической ситуации, безопасность, провокация, экстремизм, конфликт безопасности.*

Постановка проблеми. Проблема підтримання злагоди в суспільстві, забезпечення внутрішньодержавної безпеки безпосередньо пов’язана з соціальними конфліктами, які можуть провокуватись політичними процесами.

До кризових ситуацій внутрішньодержавного масштабу відносяться: громадянська війна; погіршення стану безпеки індивіда і суспільства; різке зниження рівня добробуту населення; екологічна катастрофа та ін. Кризові ситуації такого порядку, незважаючи на всю різноманітність цих ситуацій, піддаються загальному, філософському усвідомленню їх природи, що дозволяє визначити шляхи убезпечення суспільства від їх негативних наслідків, для чого в нагоді стає методологія теорії державного управління. Особливої небезпеки набувають конфлікти, які є результатом провокацій, спрямованих на дестабілізацію соціально-політичної ситуації, маючи єдине підґрунтя, злу волю ініціатора сценарію щодо негативного розвитку подій. Протистояти провокації можливо тоді, коли з’являється розуміння всієї негативності дій, спрямованих на підрив внутрішньодержавної ситуації, коли соціальна свідомість визнає їх безперечним злом для свого існування. Відповідний процес повинен відбуватися природним шляхом, без порушення соціальних зв’язків, комунікаційних каналів у суспільстві. Індивід і суспільство в цілому не повинні ставати об’єктом провокативних дій як ініціатора конфлікту, так і сторони, яка взяла на себе обов’язок забезпечувати безпеку на всій території країни шляхом захисту національних інститутів та інтересів, поваги до законів, підтримання миру та громадського порядку, захисту людей і майна.

Зловмисне провокування конфлікту, наслідком якого є дестабілізація сталого розвитку суспільства, не може залишатися поза увагою держави. Порушення нормального перебігу суспільного життя, що, по суті, є безпековим станом, повинно оцінюватись як загроза безпеці, суспільно небезпечне діяння, так як провокування насилля носить агресивний, насильницький характер.

Результати аналізу наукових публікацій. Теоретико-методологічним засадам аналізу соціальних конфліктів, їх природи, типології, функціональним наслідкам присвячено наукові розробки В. Бурлачука, А. Бандурко, Є. Головахи, О. Глухової, О. Зайцева, А. Здравомислова, О. Кабачної, В. Казакова, Т. Кільмашкіної, Ю. Мацієвського, Л. Ніковської, Н. Паніної, С. Прошанова, Л. Цой, Н. Чувашової, В. Якимець та інших учених.

Характеристика соціально-політичних конфліктів міститься в дослідженнях низки вітчизняних і зарубіжних науковців Т. Білецької, З. Голенкової, Є. Головахи, А. Дмітрієва, Т. Заславської, С. Катаєва, М. Лапіна, Д. Марковича, Ю. Саєнка, О. Стегнія, В. Степаненко та ін.

Метою статті є дослідження природи внутрішньодержавного конфлікту, який виникає в результаті провокування загострення соціально-політичної ситуації в країні.

Виклад основного матеріалу. В Україні мета протидії провокації конфлікту співпадає з проблемами державотворення. Вона полягає у здійсненні соціально-економічних, політико-правових, організаційно-структурних заходів у напрямі всебічного забезпечення потреб та інтересів громадян щодо безпеки. Саме безпеки, тому що в умовах світової економічної кризи провокація конфлікту суттєво перешкоджає проведенню економічних реформ, блокує надходження інвестицій і допомоги Міжнародного валютного фонду та руйнує процес становлення ринкових інститутів держави. Своєю чергою, економічна злочинність, насамперед організована, використовує провокацію конфлікту підживлення, створює реальну загрозу національній безпеці України, негативно впливає на соціальні, правові, політичні та міжнародні відносини. Тому, проблема ефективної протидії провокуванню конфліктів є одним із невідкладних завдань керівництва держави, органів державної влади, місцевого самоврядування й громадськості, адже дестабілізація соціально-політичної ситуації чинить руйнівний вплив на всі сфери життя суспільства.

Система реагування на провокації має бути ефективною, тому передбачається застосування різнобічних форм соціальної діяльності, соціальних технологій, всіх можливих варіантів досягнення мети найвищого порядку, визнаних у соціально-політичному аспекті справедливими і доцільними. Критерій, закладений в цю формулу, відпрацьовувався досвідом соціальної діяльності, здобутим не завжди із застосуванням наукового апарату, тобто не на засадах раціонального пізнання в чистому вигляді.

Процеси протистояння провокації, втягуванню суб’єкта соціальних відносин у конфлікт повинні виходити з характеристики відповідного феномена. Існує загально визначена негативна оцінка провокації як цілеспрямованих дій, в результаті яких свідомо погіршується стан об’єкта впливу, відбувається потрапляння його в розставлену провокатором пастку. Жоден з учасників соціальних відносин не може бути повністю убезпечений від намагань зловмисника спонукати його до дій, які можуть спричинити тяжкі наслідки. Особливо це небезпечно в політичній сфері, коли в результаті провокації відбувається дестабілізація обстановки, ескалація насильства, дискредитація політики держав, партій, лідерів, дезінформації громадської думки та ін. Використання досягнень соціальної інженерії у цілях дестабілізації ситуації робить провокацію одним із елементів сценарію досягнення зловмисником своїх цілей, в тому числі й вчинення насилля, що у такому випадку робить її суспільно небезпечним явищем.

Зміст національної безпеки в аспекті протидії дестабілізації соціально-політичній ситуації в тому, що вона в процесах регулювання суспільних відносин виступає тим загальним фактором, який об’єднує людей, критерієм оцінки соціальної інтегрованості членів суспільства, оцінки рівня справедливості суспільства.

Соціальні блага впливають на індивідів у випадках, коли, хоча і малою мірою вони збігаються з існуючими у них ідеальними моделями добра. Індивід обстоює таку точку

зору: якщо існуючі соціальні блага, шляхи їх досягнення не ефективні, не приносять бажаних результатів, то їх необхідно ліквідувати, створити нові, які будуть ефективнішими, завдяки яким буде досягнуто бажаний ідеальний результат, тобто треба ліквідувати зло і встановити справедливість. Але цих соціальних благ ще не існує в даному суспільстві. Отже, постають запитання: чому їх немає? Чия в цьому вина? Винними визнаються ті, хто не вірить у рекомендований і заявлений ними універсальний спосіб. Індивіди схиляються до вжиття заходів, які в існуючій соціальній системі вважаються злом і опиняються на позиції – “ми і самі візьмемо те, що для нас є добром”. У цьому можна виявити підстави різних видів екстремізму. Злом визнаються установи, за допомогою яких забезпечується стабільність існування самого суспільства. Негативна сторона суспільних відносин змінює свою полярність. Основи, на яких ґрунтуються суспільні відносини, що забезпечують соціальні блага, визнаються протилежними добру, при цьому можуть бути обрані засоби нових соціальних благ, які не відповідають поняттю стабільності в суспільстві. Дії окремої групи соціумів щодо дестабілізації суспільних відносин як усередині суспільства, так і поза ним можуть визнаватись ними як добро, хоча для решти суспільства це буде безперечним злом.

Екстремізм – це зло, тому що він уособлює гонитву за примарою, одним із проявів якої є застосування агресивної сили для досягнення злочинної мети, без урахування того, що досягти добра можна також шляхом реформ вже існуючих установ. Віднесення процесів, які відбуваються в суспільстві, до сфери “зла” чи “добра” є однією зі складних, необхідних умов існування суспільства як нації. Саме баланс процесів, які позначаються цими категоріями, характеризує її як розвинуту, гуманістичну, таку, що перебуває на позиціях загальнолюдських цінностей, чи, навпаки, – злочинну націю. Але такі висновки можна робити, співвідносячи свої позиції з світовим досвідом, який дістав відображення в загальнофілософських працях – носіях загальнолюдської совісті, а не спираючись тільки на суб’єктивні бачення та уявлення категорії “зло”. У той же час слід поважати право кожного соціуму і, відповідно, нації на волю совісті. Критерієм такої волі є загальнофілософська категорія “справедливість”.

До суспільних норм справедливості першого порядку відносяться норми, правила поведінки людей, без яких неможливе існування суспільства. Ці соціальні норми оціночного характеру відображають зацікавленість суспільства у підтримці порядку і регулюють моральні стосунки особи з особою. Останнє передбачає моральний мінімум взаємостосунків між “приватними особами”. Наприклад, брехня, лицемірство, агресія з давніх часів вважалися ворогом справедливості. Проблема організації управлінських процедур у сфері безпеки на засадах норм справедливості першого порядку має як етичний, так і політичний аспекти. Етика і політика невід’ємно пов’язані. Етика розкриває зміст справедливості й несправедливості, політика практично втілює в життя ці поняття.

Зворотною стороною цього процесу є деструктивність процесів, коли соціально-політичні конструкції віддалені від дійсності та людини, вони стають підґрунтям тоталітарно-догматичних програм перебудови суспільства, загального плану обману суспільства, маніпулювання ним.

Професор Д. І. Дубровський, автор монографії “Обман”, стверджує, що обман є засобом захисту і реалізації інтересів як окремих особистостей, так і груп, класів, народів і держав. Обман можна розглядати і як функції соціального інституту (державного органу, відомства, громадської організації і т.ін.). Обман може слугувати однією з форм проявів соціальних протиріч, висловлюючи егоїстичне відокремлення, конкуренцію, а також всілякі способи досягнення своїх інтересів і цілей за рахунок інших або всупереч бажанням інших. “Одна з найважливіших соціальних функцій

обману полягає в тому, що він здатний забезпечувати можливість збереження існування комунікативних структур в умовах розбіжних або практично несумісних інтересів” [1].

Обман – це напівправда, що провокує розуміння її людиною на помилкові висновки з достовірних фактів: повідомляючи деякі справжні факти, обманщик навмисне приховує інші, важливі для розуміння відомості.

Обман, як і брехня, виникає тоді, коли стикаються чиїсь інтереси і моральні норми, і там, де вдаються до обману людини ускладнене або неможливе досягнення бажаного результату іншим шляхом. “Головне, що поєднує обман з брехнею – це свідоме прагнення людини спотворити істину” [2].

При функціонуванні національної системи безпеки потрібно враховувати труднощі соціально-політичного, соціально-психологічного характеру, які може створювати її використання зі злочинною метою як для системи, так і суспільства в цілому.

Стан справ у сфері безпеки показує, що наявність сили є обов’язковою умовою для ефективної дії механізму примусу. Своєю чергою, застосування сили характеризує механізм примусу як систему підкорювання інтересів об’єктів управлінського впливу заради досягнення загальносистемної мети, якою в макросистемах безпеки виступає боротьба з насильством. Але силовий характер дії механізму примусу містить у собі небезпеку, зміст якої полягає в тому, що механізм примусу ґрунтується на засадах обмеження інтересів, а втрата частини інтересів суб’єктом суспільних відносин є основною причиною виникнення конфліктів. Зі свого боку, насильство – це засіб провадження конфлікту, тоді як конфлікт – це стан справ. Таким чином, потребує розв’язання проблема, яка полягає у моделюванні найбільш доцільних систем безпеки, функціонування яких не створювало б умов для виникнення конфліктів.

Соціологічний підхід надає можливість справитися з цією проблемою. Соціологічний аспект управління у сфері безпеки містить одне з складних питань, що пов’язане з проблемою розв’язання протиріч, які виникають в процесі здійснення управлінського впливу державою як суб’єкта управління й соціуму і соціальних систем як об’єкта управлінського впливу. Суспільство є складною системою, тобто системою, яка складається з великої кількості елементів, об’єднаних соціальними зв’язками. Соціум як основний суб’єкт і об’єкт цієї системи є носієм певних цілей, позицій, поглядів, котрі мають як суб’єктивний, так і об’єктивний характер. Об’єктивні компоненти існування індивіда об’єднуються поняттям “потреба”, суб’єктивні – поняттям “інтерес”. Обидва види понять розглядались вище і зроблено відповідні висновки. Водночас, для того щоб ефективно керувати системою внутрішньодержавної безпеки, потрібно встановити взаємозалежність не тільки між поняттями, що належать до однієї групи соціальних зв’язків, але й між тими, які мають різну природу, протиріччя, і разом з тим об’єктивно зумовлюють взаємозалежність свого існування. Зіткнення протилежних цілей, позицій, поглядів суб’єктів потреби й інтересу безпеки можна прийняти як конфлікт між об’єктивними і суб’єктивними системами соціальної безпеки. Такого роду протиріччя у сфері безпеки припустимо розглядати у соціально-правовому аспекті, що передбачає соціально-управлінську характеристику конфлікту. Саме така характеристика конкретизує і пояснює природу протиріч, які можна віднести до сфери безпеки. Причини протиріч як джерела конфлікту полягають у соціальній неоднорідності суспільства, розбіжностях у рівні доходів, влади, престижу і т. ін. Виходячи з цих ознак, можна розглянути конфлікт у соціально-управлінському аспекті.

В узагальненому розумінні конфлікт – це поширене явище, якому даються різні пояснення. Найбільш змістовне його пояснення знаходимо у визначенні англійського соціолога Е. Гіуддєнса: “Під конфліктом я маю на увазі реальну боротьбу між діючими

людьми чи групами, незалежно від того, які джерела цієї боротьби, її способи і засоби, що мобілізуються кожною зі сторін” [3, с. 106].

У нашій країні склалась традиція пояснення конфліктів через об’єктивні протиріччя інтересів великих соціальних груп, які диктують сторонам логіку, тривалість, ступінь напруженості боротьби щодо задоволення суттєвих потреб. В обох підходах визнається, що конфлікт пов’язаний з процесом боротьби, яку автори наукових досліджень розуміють в аспекті протистояння інтересів чи потреб. Розбіжності з цього питання для нас мають значення в аспекті визначення конфлікту у сфері безпеки як протистояння об’єктивного і суб’єктивного. З’ясуємо цю тезу з теоретико-управлінської позиції.

Як уже зазначалось, процес боротьби є невід’ємною частиною суспільного життя, але виникає питання: чи можна розцінювати конфлікт як боротьбу і чи існує між цими поняттями різниця? Вирішення питання знову ж полягає у встановленні взаємозалежності потреби індивіда з інтересами соціуму, які за наявності протиріч утворюють конфліктну ситуацію у сфері безпеки. Це питання важливе тому, що критерій об’єктивності визначає цілі соціальних систем, які відповідають за забезпечення безпеки в суспільстві.

Питання такого порядку розглядаються у самостійному напрямі наукових досліджень, який дістав назву “державно-правова конфліктологія”. Завданням державно-правової конфліктології є вивчення конфліктів у соціально-політичній сфері суспільних відносин. Соціально-правові конфлікти мають своїми підвалинами соціально-економічні, соціально-політичні чинники інтересу безпеки. До причин їх виникнення, на наш погляд, відносяться: протиріччя, пов’язані з обстоюванням інтересів у сферах виробництва, технології розподілу, обміну; протиріччя, пов’язані з обстоюванням класових, національних, етнічних, соціально-групових інтересів (ліберальний підхід); протиріччя, пов’язані з обстоюванням інтересів у сфері духовного життя, – моральні, релігійні, художньо-естетичні, наукові; протиріччя, пов’язані з обстоюванням інтересів в культурно-побутовій сфері, – побутові, родинно-сімейні, товариські тощо.

Конфлікт, пов’язаний з обстоюванням інтересу безпеки, має чітко визначений суб’єктивний, тобто соціально-психологічний характер. Конфлікт такого роду може бути визначений в різних аспектах: як явище міжособистісних і групових відносин; зіткнення тенденцій, оцінок, принципів, думок, характерів, еталонів поведінки; прагнення людей до ствердження ідеї, яку вони захищають, принципу, вчинку; деструкція міжособистісних відносин на емоційному, когнітивному чи поведінському рівні; форма комунікації людини з людиною, людини з групою людей або її частиною, однієї частини колективу з іншою, колективу з колективом; захист і водночас реакція у відповідь на вплив; реакція на несприятливі ситуації, що травмують особистість, на перешкоди у досягненні яких-небудь цілей; дезінтегруюча сила людських відносин, а її подолання – інтегруюча сила; один із засобів самоутвердження, подолання перешкоджаючих особистості тенденцій.

Наявність у людини, суспільства інтересу безпеки, зумовлює необхідність визнання процедур розв’язання конфліктів з позиції їх суб’єктивності, для чого визначаються шляхи консолідації суспільства і сприяння соціальній злагоді. Врегулювання конфліктів з позиції суб’єктивної природи мають достатньо широке коле дослідження в різних теоріях.

У полеміці між представниками різних соціальних теорій категорія конфлікту часто стає імпульсом до створення конфліктуючих таборів (теорія конфлікту Райнера Претроіуса). Це особливо характерно для політичної соціології, яка у США у 1960-х роках розпалась на два блоки: “конфліктну школу” і “школу конфлікту”.

Лоренц фон Штайн сформулював концепцію, дотримуючись примата діяльності держави, що регулює через апарат управління кризові ситуації шляхом досягнення

компромісів; Еміль Дюркгейм висунув теорію індивідуалізації конфліктних ситуацій на базі розподілу праці й соціальної діяльності.

Цей напрям представляють автори, інтереси яких (особливо між послідовниками Дюркгейма) переважно зосереджені на розробці концепції індивідуалізації і дисперсії (розпиленні) конфлікту. Згідно з їхніми поглядами, протиріччя, врешті-решт, відносяться до орієнтацій і дієвих установок самих суб’єктів. Відповідно, арбітраж і баланс (інтересів) необхідно шукати саме в суб’єктах. Об’єктивність протиріч у сфері реалізації потреби безпеки полягає у відношенні між правовою формою діяння та його матеріальною соціально-політичною сутністю.

З часом висування і поширення перерахованих концепцій політичної теорії конфлікту розвивались за двома напрямами. До першого з них належать теоретики, які дотримуються поглядів К. Маркса. Конфлікт в суспільстві вони розглядають як конфронтацію великих соціальних груп, класів. Тому ці теоретики зосереджують свою увагу на макросоціальних вимірах, які полягають у виявленні й дослідженні фундаментальних протиріч і співвідношень інтересів тих чи інших сил. Як правило, прихильників цього напряму об’єднує зацікавленість у зміні існуючої системи, а звідси випливає їх концепція про перетворення суспільства взагалі.

Таким чином, якщо в першому напрямі його представники висувають концепцію “приватизації” конфлікту, нормативна перевага тут найчастіше віддається соціальній стабільності й збереженню основної системи, то представники другого напряму приділяють увагу виявленню конфлікту на стадії “політизації”, в його колективному виявленні – через групи і класи.

Соціально-правова сфера, особливо в перехідний період, не може бути безконфліктною. Безконфліктність – це шлях, який веде до стагнації політичного життя, соціально-політичних відносин, внутрішньодержавного законодавства. Все це потребує вивчення механізмів розв’язання конфліктів, які виникають при забезпеченні інтересів безпеки, нейтралізації їхніх негативних наслідків. Цієї мети можна досягти, якщо поєднати обидва напрями розвитку теорії розв’язання конфліктів, що дає можливість встановлення зв’язку – об’єктивного і суб’єктивного – в конфлікті безпеки.

Висновки.

Провокування внутрішньодержавного конфлікту можна віднести до явища, яке має суб’єктивну природу для суб’єкта інтересу безпеки та об’єктивну – для суб’єкта потреби безпеки. Таким чином, ми встановлюємо зв’язок процесу відстоювання інтересу безпеки і потреби безпеки з поняттям конфлікту безпеки. Конфлікт безпеки – це протиріччя між потребою в безпеці та інтересами, характер яких визначається злою волею суб’єктів.

Таким чином, дестабілізація соціально-політичної ситуації є провокацією внутрішньодержавного конфлікту та загрозою безпеці як індивіда, так і суспільства в цілому.

Використана література

1. Дубровский Д.И. Обман. Философско-психологический анализ / Д.И. Дубровский. – [2-е изд., доп.]. – М. : Канон + РООИ “Реабилитация”, 2010. – 336 с.

2. Знаків В. В. Макіавеллізм і феномен брехні // Питання психології. – 1999. – № 6. – С. 59-70.

3. Радугин А.А., Радугин К.А. Социология: курс лекций / А.А. Радугин, К.А. Радугин. – М. : Владос, 1995. – 192 с.

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

УДК: 342.1+355/359

БОЛДИР С.В., начальник Департаменту охорони державної таємниці та ліцензування Служби безпеки України

ПЕРСПЕКТИВИ РЕФОРМУВАННЯ СИСТЕМИ ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ ТА СЛУЖБОВОЇ ІНФОРМАЦІЇ

Анотація. *У статті на основі наявного досвіду та проведеного аналізу норм законодавства іноземних держав у сфері безпеки інформації розкриваються окремі питання, пов’язані з практичними аспектами реалізації вказівок керівництва держави, задекларованих у різних нормативних актах щодо реформування національного законодавства у згаданій сфері діяльності.*

Ключові слова: *реформування законодавства, система охорони державної таємниці та службової інформації, безпека інформації, стандарти НАТО та ЄС.*

Summary. *The article discloses certain questions related to practical aspects of implementation of the state leadership instructions declared in various normative acts, concerning the reform of the national legislation in the mentioned area of activity, based on actual experience and analysis of the legislative acts in the sphere of information security of foreign countries .*

Keywords: *legislation reforming, system of protection of state secrets and official information, information security, NATO and EU standards.*

Аннотация. *В статье на основе имеющегося опыта и проведенного анализа норм законодательства иностранных государств в сфере безопасности информации раскрываются некоторые вопросы, связанные с практическими аспектами реализаций указаний руководства государства, задекларированных в различных нормативных актах по реформированию национального законодательства в упомянутой сфере деятельности.*

Ключевые слова: *реформирование законодательства, система охраны государственной тайны и служебной информации, безопасность информации, стандарты НАТО и ЕС.*

Постановка проблеми. Одним із пріоритетних напрямів державної політики національної безпеки України, виходячи із положень Стратегії національної безпеки України, яку затверджено Указом Президента України від 26.05.2015 № 287/2015, є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів Організації Північноатлантичного договору та Європейського Союзу [1].

Необхідність формування нових підходів до забезпечення функціонування вказаної системи зумовлена передусім взятим Україною курсом на інтеграцію у світове співтовариство та розширенням міжнародного співробітництва у політичній, оборонній, науково-технічній та інших сферах діяльності, а також певною фізичною та моральною застарілістю національного законодавства у сфері охорони інформаційних ресурсів, сформованого значною мірою на основі нормативних актів колишнього СРСР.

При цьому закритість сфери охорони державної таємниці призвела до збереження у своїй основі засад побудови та функціонування радянського механізму захисту державних секретів, який утратив свою ефективність і перестав відповідати сучасним реаліям, що суттєво вплинуло на принципи захисту інформації [2, с. 335].

З урахуванням викладеного та зважаючи на важливість зазначеного питання, яке безпосередньо стосується національної безпеки України, очевидним є те, що впровадження певних новацій потребує виваженого підходу та ретельного вивчення практики їх застосування в інших державах.

Результати аналізу наукових публікацій. Дослідженню питань, пов’язаних з реформуванням системи охорони державної таємниці та службової інформації, присвячені роботи таких науковців як С. Князєва, І. Мейдича, О. Розвадовського, О. Семенюка, В. Шлапаченка та інших. Проте і на сьогодні, у зв’язку з відсутністю єдиного державного бачення щодо шляхів реалізації певних реформаторських започаткувань, окреслена проблема не отримала належного теоретичного осмислення.

Метою статті є аналіз сучасного стану системи охорони державної таємниці та іншої інформації з обмеженим доступом з урахуванням практики держав-членів НАТО та ЄС, окреслення основних перспективних шляхів її удосконалення для кардинального підвищення ефективності національних спроможностей щодо забезпечення гарантованого рівня безпеки таких відомостей.

Виклад основного матеріалу. Цілком зрозуміло, що визначенню основних перспективних напрямів реформування системи охорони державної таємниці та службової інформації має передувати вивчення досвіду держав-учасниць НАТО та ЄС з розбудови та впровадження дієвої системи захисту інформації. Результати опрацювання цього питання засвідчили, що національне законодавство таких країн у цій сфері базується на мінімальних стандартах безпеки, встановлених зазначеними міжнародними організаціями.

Тому, поряд з розглядом національних нормативно-правових актів держав євроатлантичної спільноти, ґрунтовного вивчення та дослідження вимагають підходи до захисту інформації саме НАТО та ЄС, оскільки, як влучно зазначив Розвадовський О.Б., вони є результатом спільних зусиль, формувалися під впливом і за участю розвинутих країн світу, містять обов’язкові для всіх країн-членів універсальні приписи [3, с. 163].

Аналіз іноземної нормативної бази довів, що вітчизняне законодавство у сфері охорони державної таємниці та службової інформації не повною мірою узгоджується зі стандартами безпеки НАТО та ЄС, що може вплинути як на міжнародні партнерські взаємовідносини у сфері захисту інформації, так і ускладнити інтеграційні процеси нашої держави.

На наш погляд, одним із найважливіших напрямів, за яким має здійснюватися реформування української системи охорони державної таємниці та службової інформації, є кардинальний перегляд “філософії” віднесення інформації до такої, що потребує обмеження у доступі.

На сьогодні первісним законодавчим актом, що регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, є Закон України “Про інформацію”, який, зокрема, визначає порядок доступу до інформації, поділяючи її на відкриту та з обмеженим доступом [4].

Разом з тим, у контексті впливу зовнішніх та внутрішніх чинників на стале функціонування держави найбільш уразливою є інформація, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України “Про доступ до публічної інформації” [6], та яка підлягає охороні державою, тобто державна таємниця та службова інформація.

Водночас, на сьогодні склалась ситуація, коли недостатнє нормативно-правове врегулювання окремих аспектів захисту інформаційних ресурсів призвело до значної втрати впливу держави на забезпечення схоронності саме службової інформації.

Як зазначив Мейдич І.М., визначення службової інформації в законодавстві України на сьогодні відсутнє. У ст. 9 Закону України “Про доступ до публічної інформації” подається лише перелік відомостей (до того ж не вичерпний), які можуть до неї належати, який не містить чітких критеріїв віднесення інформації до службової.

Узагальнений Перелік відомостей, що становлять службову інформацію (на кшталт ЗВДТ), законодавством не передбачений. Відомості, що становлять службову інформацію, у відомчих переліках визначаються без чіткої структуризації та недостатньо конкретно. Зазначені чинники не сприяють правильному встановленню службової інформації, як предмета кримінально-правової охорони [5, с. 164].

Дійсно, згідно з положеннями наведеного законодавчого акта відомості, що становлять службову інформацію, визначаються у відповідних переліках, які складаються органами державної влади, органами місцевого самоврядування, іншими суб’єктами владних повноважень, у тому числі на виконання делегованих повноважень [6].

Проте, на законодавчому рівні єдині вимоги щодо таких переліків не встановлені, тому розпорядники інформації відносять її до службової, у більшості випадків, на свій розсуд. При цьому контроль за цим процесом здійснюється лише для інформації, зібраної в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Відсутність належної уваги з боку суб’єктів владних повноважень до процедури складання переліку відомостей, що становлять службову інформацію, може викликати безпідставне оприлюднення зазначеної інформації та завдати значної шкоди національній безпеці держави, а також призвести до порушення конституційних прав та свобод людини і громадянина.

Тому, першочерговим є вирішення питання щодо впровадження нових комплексних підходів та створення уніфікованої системи безпеки як державної таємниці, так і службової інформації, яка б забезпечувала в усіх сферах надійний та ефективний захист чутливих відомостей, спеціальний режим доступу до яких встановлюється, виходячи з інтересів держави.

Слід зазначити, що така позиція співпадає з висновками Мейдича І. М., на думку якого ґрунтовною проблемою удосконалення кримінально-правової охорони службової інформації є переосмислення її статусу як виду таємної інформації та закріплення в законодавстві її визначення, за аналогією з державною таємницею, яке б конкретизувало її тлумачення та сприяло правильній кваліфікації як предмету злочинних посягань [5, с. 164].

Безумовно, при вирішенні цього проблемного питання має бути враховано, що у стандартах безпеки НАТО та ЄС, а також нормативній базі більшості країн-членів цих міжнародних організацій відсутні поняття “державна таємниця”, “службова інформація”, натомість передбачено застосування єдиного терміну для позначення відомостей з еквівалентними ступенями обмеження доступу, а саме – “classified information”, прямим перекладом якого є “класифікована інформація” (саме у такому написанні вказаний термін поширено використовується в україномовних ресурсах).

Зокрема, на нормативному рівні впроваджено чотирьохрівневу систему обмеження доступу до вказаної інформації, ступені якої розподіляються за рівнем шкоди, яку може бути заподіяно інтересам міжнародних організацій та країн-членів у разі розголошення класифікованих відомостей [7; 8].

З огляду на викладене, вбачається, що закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів та процедур щодо застосування системи ступенів обмеження доступу до інформації дозволить демократизувати цей процес, забезпечивши його прозорість, сприятиме оптимізації роботи з визначення ступенів секретності матеріальних носіїв інформації, а також гармонізації та адаптації національного законодавства до вимог політики безпеки євроатлантичного суспільства.

Саме тому, з метою виокремлення секретної та службової інформації з-поміж інших категорій інформації з обмеженим доступом (до яких відноситься конфіденційна та інша таємна інформація, що містить професійну, банківську таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю), пропонується об’єднати державну таємницю та службову інформацію в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6 Закону України “Про доступ до публічної інформації” [6], та яка підлягає охороні державою.

При цьому, з огляду на відсутність у законодавстві України аналогу впровадженого у стандартах безпеки НАТО та ЄС терміну “класифікована інформація”, еквівалентне поняття, що відповідатиме належному його розумінню з урахуванням традиційних та сталих форм застосування (наприклад “засекречена інформація”, “секретна інформація”) має бути закріплено на законодавчому рівні.

Поряд із цим, потребують правового врегулювання й інші питання у сфері безпеки інформації, зокрема, визначення на законодавчому рівні Національного органу безпеки.

Відповідно до стандартів безпеки НАТО та ЄС однією з умов євроатлантичної інтеграції держав-партнерів в загальноєвропейську систему обміну інформацією з обмеженим доступом є створення Національного органу безпеки [7; 8].

Так, згідно з вимогами стандартів безпеки НАТО та ЄС у державах-учасницях створюються Національні органи безпеки, основною функцією яких є впровадження стандартів безпеки інформації, здійснення інспектувань умов захисту інформації з обмеженим доступом у всіх національних організаціях на всіх рівнях, забезпечення проведення перевірки з визначення надійності громадян, які потребують доступу до секретної інформації, видачу дозволів на провадження діяльності, пов’язаної з інформацією з обмеженим доступом [7; 8].

Статус та підпорядкованість такого органу визначаються державами-учасницями вказаних міжнародних організацій самостійно з урахуванням традиційних підходів та практики забезпечення охорони інформації з обмеженим доступом.

Поширеною є також практика створення Національних органів безпеки при окремих державних органах (при Міноборони – Великобританія, Естонія, Кіпр, Норвегія, Франція; Нідерланди, при МЗС – Бельгія, Фінляндія, Швеція, при МВС – Німеччина, при Раді Міністрів – Італія, Португалія). У деяких країнах функції Національних органів безпеки покладаються на національні спецслужби (Греція, Польща, Румунія – законодавство гармонізовано зі стандартами НАТО та ЄС) або діяльність такого органу скеровується керівником спеціальної служби (Іспанія).

Разом з тим, статтею 2 Адміністративних домовленостей щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного договору на Службу безпеку України як орган безпеки покладено впровадження мінімальних стандартів охорони та поводження з такою інформацією, обмін якою здійснюється між Україною та НАТО, узгоджених у цих Домовленостях, та забезпечення нагляду за їхнім дотриманням [9].

Водночас, вказане має знайти своє відображення, як цього вимагають стандарти безпеки НАТО, у національному законодавстві у сфері охорони державної таємниці в частині визначення Служби безпеки України як Національного органу безпеки.

Відповідно до стандартів безпеки НАТО та ЄС, окрім забезпечення виконання усіх заходів та процедур безпеки, а також контролю за охороною інформації, обмін якою здійснюється, передбачено наділення Національного органу безпеки функціями з комунікаційно-інформаційної безпеки, у т.ч. і з питань технічного захисту інформації [7; 8].

Вказаний підхід, на нашу думку, сприяє ефективному вирішенню нагальних завдань у сфері безпеки інформації, створює необхідні умови для удосконалення державного контролю і координації діяльності державних органів з питань технічного захисту інформації.

У свою чергу, в Україні питання щодо реалізації державної політики у сферах криптографічного та технічного захисту інформації наразі покладено на Державну службу спеціального зв’язку та захисту інформації України [10].

При цьому забезпечення охорони державної таємниці відповідно до статті 2 Закону України “Про Службу безпеки України” покладається на Службу безпеки України у межах визначеної законодавством компетенції [11].

Так, дійсно: покладання повноважень з питань забезпечення технічної та криптографічної складової охорони державної таємниці на інший орган свідчить про комплексний підхід до забезпечення охорони державної таємниці. Однак в умовах протистояння збройній агресії Російської Федерації на сході України функціональна розгалуженість з питань охорони державної таємниці, зокрема неналежне забезпечення технічного захисту інформації може призвести до значного погіршення ефективності функціонування загальнодержавної системи охорони державної таємниці.

Слід наголосити, що невідповідність стану технічного захисту інформації вимогам сьогодення може призвести до суттєвого підвищення уразливості інформації з обмеженим доступом, яка накопичується, зберігається й обробляється в автоматизованих системах, через що спостерігається зростання загроз безпеці держави, суспільства та особистості.

Тому впровадження ефективних заходів з технічного захисту інформації, як невід’ємної складової охорони інформації з обмеженим доступом, сприятиме надійному функціонуванню системи національної безпеки держави. З огляду на викладене, пропонується запровадити нові підходи до визначення повноважень державних органів з функцій контролю за технічним захистом інформації у сфері охорони державної таємниці.

Крім того, потребують удосконалення і такі напрями охорони державної таємниці, як порядок провадження діяльності, пов’язаної з державною таємницею, процедури перевірки громадян у зв’язку з допуском до державної таємниці, а також питання впровадження диференційованих підходів до застосування фізичних та технічних заходів захисту інформації залежно від наданого грифу обмеження доступу до інформації. Виклад вказаної проблематики є достатньо осяжним, у зв’язку з чим доцільно продовжити науковий дискурс концептуальних питань реформування системи охорони державної таємниці та службової інформації.

Висновки.

Система охорони державної таємниці та службової інформації потребує постійного удосконалення, оскільки виклики сьогодення, у т.ч. і в інформаційній сфері, вимагають якнайшвидшого реагування та протидії. Відповідно, робота щодо виокремлення саме “чутливих” напрямів охорони державної таємниці та службової інформації, які потребують змін, має проводитися пропорційно розвитку у сфері інформаційної безпеки.

Зокрема, основні зусилля у ході здійснення заходів з реформування системи охорони державної таємниці та службової інформації мають бути зосереджені на вирішенні наступних питань:

- об’єднання державної таємниці та службової інформації в єдину категорію інформації, доступ до якої обмежується виключно в інтересах, передбачених статтею 6

Закону України “Про доступ до публічної інформації”, та яка підлягає охороні державою; здійснення заходів щодо впровадження нових комплексних підходів та створення уніфікованої системи безпеки як державної таємниці, так і службової інформації, яка б забезпечувала в усіх сферах надійний та ефективний захист чутливих відомостей, спеціальний режим доступу до яких встановлюється, виходячи з інтересів держави;

- закріплення на законодавчому рівні встановлених політикою безпеки НАТО та ЄС стандартів та процедур щодо застосування системи ступенів обмеження доступу до інформації;
- визначення у вітчизняному законодавстві у сфері охорони державної таємниці Служби безпеки України як Національного органу безпеки.

Крім того, враховуючи, що на Службу безпеки України покладено впровадження мінімальних стандартів безпеки НАТО та ЄС, пропонується запровадити нові підходи до визначення повноважень державних органів з функцій контролю за технічним захистом інформації у сфері охорони державної таємниці.

Також слід зазначити, що наведені пропозиції щодо реформування системи охорони державної таємниці та службової інформації узгоджуються з напрацюваннями та висновками робочої групи, за результатами діяльності якої розроблено пропозиції до проектів Концепції реформування системи охорони державної таємниці та службової інформації, а також відповідних нормативних актів щодо введення її у дію в рамках виконання пункту 4.12 Стратегії національної безпеки України, затвердженої Указом Президента України від 26.05.2015 р. № 287/2015 [1], а також задля усунення наявних розбіжностей у підходах до захисту інформації з обмеженим доступом у державах євроатлантичної спільноти та в Україні.

Переконані, що реалізація зазначених напрямів має здійснюватися на підставі ґрунтовного вивчення досвіду країн євроатлантичної спільноти щодо охорони їх класифікованої інформації.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України” : Указ Президента України від 26.05.15 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/287/2015

2. Семенюк О.Г. Проблеми охорони державної таємниці: кримінально-правові та кримінологічні аспекти : монографія / О.Г. Семенюк. – К. : “Видавничий дім “АртЕк”, 2017. – С. 335.

3. Розвадовський О.Б. Забезпечення охорони державної таємниці та службової інформації: теоретичний, правовий та організаційний аспекти : моногр. : у 2-х ч. – Ч. 1 / О.Б. Розвадовський. – К. : Центр навч.-наук. та наук.-практ. видань НА СБ України, 2014. – С. 163.

4. Про інформацію : Закон України від 02.01.92 р. № 2658-XII. – Режим доступу : http://zakon.rada.gov.ua/laws/show/2657-12

5. Мейдич І.М. Кримінально-правова охорона службової інформації : підходи до удосконалення : матеріали науково-практичної конференції, 08 червня 2016 р. ; упорядн. В.М. Фурашев, С.Ю. Петряєв., 2016. – С. 164.

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

7. Security within the North Atlantic Treaty Organisation (C-M(2002)49). – Режим доступу : http://arhives.nato.int/amendments-to-nato-c-m-55-15-final;isad

8. Council Decision of 23 September 2013 on the security rules for protecting EU classified information (2013/488/EU). – Режим доступу : http://publications.europa.eu/en/publication-detail/-/publication/d43001e3-356d-11e3-806a-01aa75ed71a1

9. Адміністративні домовленості щодо охорони інформації з обмеженим доступом між Урядом України та Організацією Північноатлантичного договору : ЗаконУкраїни від 24.05.17 р. № 2068-VIII . – Режим доступу : http://zakon5.rada.gov.ua/laws/show/950_035-16

10. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23.02.06 р. № 3475-І. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/3475-15

11 Про Службу безпеки України : Закон України від 25.03.92 р. № 2230-XII. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2229-12

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

УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор***,** директор Навчально-наукового Інституту перепідготовки та підвищення кваліфікації кадрів СБУ Національної академії Служби безпеки України

ПИТАННЯ ЕФЕКТИВНОСТІ ДІЯЛЬНОСТІ ДЕРЖАВНИХ ОРГАНІВ У СФЕРІ ЗАХИСТУ ІНФОРМАЦІЙНОГО ПРОСТОРУ УКРАЇНИ

Анотація. *У статті досліджуються питання оцінки ефективності діяльності державних органів у сфері захисту національної інформаційної сфери. Зроблено висновок, що таку оцінку варто здійснювати шляхом проведення соціологічних досліджень з питань поінформованості українського суспільства і міжнародної спільноти про здійснювані державними органами заходи, а також їх сприйняття і підтримки.*

Ключові слова*: інформаційний простір, державні органи, ефективність діяльності, інформаційна агресія, захист інформаційного простору України.*

Summary*. The article deals with the issues of assessing the efficiency of state bodies in the field of protection of the national information sphere. It was concluded that such an assessment should be carried out through sociological research on the awareness of Ukrainian society and the international community about measures taken by state authorities, as well as their perceptions and support.*

Keywords*: information space, state bodies, efficiency of activity, information aggression, protection of information space of Ukraine.*

Аннотация*. В статье исследуются вопросы оценки эффективности деятельности государственных органов в сфере защиты национальной информационной сферы. Сделан вывод, что такую оценку следует осуществлять путем проведения социологических исследований по вопросам осведомленности украинского общества и международного сообщества об осуществляемых государственными органами мерах, а также их восприятия и поддержки.*

Ключевые слова*: информационное пространство, государственные органы, эффективность деятельности, информационная агрессия, защита информационного пространства Украины.*

Постановка проблеми. Одну з найбільших загроз національній безпеці нашої держави на сьогодні становить інформаційна агресія Російської Федерації, основою якої є продукування і поширення неправдивої інформації з метою маніпулювання суспільною свідомістю. Інформаційний вплив РФ спрямований на підрив української державності та здійснюється з метою дестабілізації ситуації в Україні, протидії євроінтеграційному курсу та мінімізації міжнародної підтримки, легітимізації самопроголошених утворень “ДНР/ЛНР” та анексії Криму.

Масштабна інформаційна агресія у вітчизняному та світовому інформаційних просторах полягає у поширенні деструктивного контенту, викривленої інформації про процеси в Україні, повідомлень тенденційного характеру, дестабілізації суспільно-політичної обстановки, інспірування сепаратистських настроїв, міжетнічної та міжконфесійної ворожнечі, розповсюдження автономістських ідей тощо. Для здійснення інформаційного впливу на населення України формується агресивна інформаційна політика російських ЗМІ, а також опосередковано залучаються до антиукраїнської діяльності вітчизняні суб’єкти інформаційного простору та контрольовані РФ іноземні засоби масової інформації.

На сьогодні актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері на державному рівні визнаються:

– здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;

– поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [1].

Результати аналізу наукових публікацій свідчать про те, що питання ефективності діяльності державних органів у сфері захисту інформаційного простору України не часто були предметом дослідження. У вітчизняній юридичній літературі дослідженню окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як І. Арістова, О. Баранов, В. Брижко, Р. Калюжний, В. Пилипчук, М. Швець та інші. Автор розглядав дотичні питання захисту інформаційних ресурсів держави [2].

Метою статті є науково-теоретичне обґрунтування підходів до визначення ефективності діяльності державних органів України у сфері захисту національного інформаційного простору.

Виклад основного матеріалу. Для формулювання підходів до визначення ефективності діяльності державних органів України у сфері захисту національного інформаційного простору проаналізуємо їх роботу за 2017 рік.

Зважаючи на нормативно закріплені загрози національним інтересам та національній безпеці України в інформаційній сфері, насамперед зосередимося на протидії державними органами виявленим механізмам впливу на інформаційну сферу України з боку держави-агресора. Для цього згрупуємо їх з урахуванням компетенції Національної ради України з питань телебачення і радіомовлення (далі – Нацрада), Міністерства інформаційної політики та Держкомтелерадіо України.

1. Системне поширення антиукраїнської пропаганди через підконтрольне службам РФ телебачення та радіомовлення.

Результативність протидії цій загрозі у 2017 році визначається наступними здобутками. Так, 17 березня 2017 р. в с. Чонгар Херсонської області відкрито 150-метрову телекомунікаційну вежу, побудовану для організації українського мовлення на територію Автономної Республіки Крим.

4 серпня 2017 року завершено монтаж нової 134-метрової вежі, яка знаходиться неподалік села Бахмутівка Новоайдарського району Луганської області. Завдяки запуску

Бахмутівської вежі аудиторія українських телеканалів та радіостанцій в Луганській області зросте до 85 – 90 тис. Охоплення населення сигналом українських радіостанцій збільшиться на 102 %, аналогового телебачення – більш ніж на 450 %, повернеться українське цифрове телевізійне мовлення в стандарті DVB-T2.

Також, для донесення сигналу українських телерадіокомпаній на захоплені території шляхом встановлення додаткових передавачів та антено-фідерних систем на радіотехнічних об’єктах Концерну РРТ здійснено наступні заходи: встановлено 20 аналогових телевізійних передавачів; встановлено 1 цифровий передавач потужністю 1 кВт; збільшено в 10 разів потужність 3 передавачів; введено в дію 21 радіомовний РМ-передавач.

Нацрада (з липня 2014 року по серпень 2017 року) за результатами моніторингів визначила іноземні програми, які містили інформацію, що порушує українське законодавство та положення Європейської конвенції про транскордонне телебачення. Виконуючи свої повноваження, які передбачені діючим законодавством, регуляторний орган ухвалив рішення, якими встановлено обмеження щодо розповсюдження на території України 80 іноземних програм.

За ретрансляцію програм, які не входять до переліку іноземних програм, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення [3] і законодавства України (статті 42 Закону України “Про телебачення і радіомовлення”), санкцію “стягнення штрафу” застосовано до 4 ліцензіатів. Впродовж 2017 року виявлено два факти ретрансляції заборонених телеканалів.

8 листопада 2016 року набув чинності Закон України “Про внесення змін до деяких законів України щодо частки музичних творів державною мовою у програмах телерадіоорганізацій” [4], яким передбачено, що упродовж першого року з моменту набуття чинності частка пісень державною мовою має становити 25 відсотків, з другого року – 30 відсотків, з третього року ця частка повинна зрости до 35 відсотків. Водночас, протягом першого року мінімальна частка ведення передач державною мовою має становити не менше 50 %, протягом другого року – не менше 55 % та з третього року – не менше 60 %. Квоти на радіо накладають на мовників зобов’язання транслювати певний контент у визначених обсягах (межах) впродовж визначеного проміжку часу. Такі вимоги встановлюються з метою захисту національного продукту.

За порушення квот на україномовні пісні та ведення програм державною мовою, які передбачені вимогами частинами 2 та 5 статті 9 Закону України “Про телебачення і радіомовлення” [5], застосовано санкцію “накладення штрафу” до 15 ліцензіатів.

Нацрадою спільно із зацікавленими державними органами (Міністерство інформаційної політики, Мінкульт, Держкіно) постійно здійснюється вивчення та вжиття відповідних заходів реагування в питаннях трансляції заборонених кінофільмів і серіалів, вироблених країною-агресором після 1 січня 2014 року, фільмів, які порушують законодавство про декомунізацію, кіновідеопродукції за участі осіб, які загрожують національній безпеці України тощо [6].

Протягом багатьох років проблема мовлення громад та критичний стан сфери проводового мовлення, яка використовується, насамперед, комунальними підприємствами, залишалася невирішеною. З метою врегулювання цього питання, Нацрадою започатковано загальнонаціональний проект заміщення застарілої проводової технології на мовлення в FM-діапазоні.

29 червня 2017 року Нацрадою було оголошено конкурс на вільні радіоканали та затверджено відповідні конкурсні умови. Однією з ключових умов цього конкурсу були вимоги до програмної концепції, зокрема, в загальному обсязі власного мовлення

радіоорганізації інформаційні передачі місцевої тематики мають становити не менше 15 відсотків, а також повинна бути передбачена можливість ретрансляції виключно програм суспільного мовлення. Позиція Нацради полягає в тому, що саме такий підхід сприятиме розвитку місцевого мовлення, зробить додатковий внесок у розбудову та захист національного телерадіопростору нашої держави.

Нацрада в межах компетенції та в рамках діяльності Комісії з питань забезпечення стабільного функціонування системи національного телебачення і радіомовлення (Комісія, очолює МІП та Міністерство з питань тимчасово окупованих територій та внутрішньо переміщених осіб України) сприяє відновленню трансляції українських теле- та радіопрограм в зоні проведення антитерористичної операції та на територію тимчасово окупованої Автономної Республіки Крим.

На підконтрольних українській владі територіях Донецької та Луганської областей відповідно до чинних ліцензій задіяно 63 частотних присвоєння для радіомовлення, 126 частотних присвоєнь для аналогового телевізійного мовлення, 44 частотні присвоєння для цифрового наземного телевізійного мовлення [6].

У зв’язку із припиненням розрахунку нових частотних присвоєнь для аналогового телевізійного мовлення, зумовлену переходом країн Європи на цифрові стандарти мовлення, а також через негативні результати міжнародної координації будь-яких українських частотних присвоєнь Адміністрацією зв’язку Російської Федерації, з метою забезпечення українським мовленням територій проведення антитерористичної операції органами частотного планування були запропоновані до використання так звані “тимчасові” телерадіоканали.

У межах поточної діяльності Комісії з метою розвитку телекомунікаційної інфраструктури реалізується проект зі збільшення висоти РТПС “Чаплинка” (смт Чаплинка Херсонської області) з 92 до 130 м (оператор телекомунікацій – Концерн РРТ). Також вивчається питання побудови нової висотної споруди у смт Попасна Луганської області, що дозволить забезпечити українським мовленням дві третини білих плям у покритті прилеглих до зони АТО територій.

Разом з тим, завершується проект щодо збільшення потужності телевізійних каналів у м. Херсоні та с. Василівка з 2,5 до 5 кВт, на яких здійснює мовлення НСТУ (UA:Перший). Оператором телекомунікацій виступає Концерн РРТ.

Відповідно до рішення Нацради від 17.08.2017 року № 1423 УДЦР замовлено перенос частотних присвоєнь РЕЗ з м. Джанкою, м. Красноперекопську та м. Євпаторії АР Крим до с. Чонгара та смт Чаплинки Херсонської області для організації радіо- та телевізійного мовлення [6].

2. Використання Інтернет-ресурсів для поширення антиукраїнської інформації, що порушує чинне законодавство України та спрямоване на розпалювання ворожнечі, закликає до повалення існуючого ладу, пропагує насильство тощо.

У Міністерстві інформаційної політики України розроблено Перелік Інтернет-ресурсів з інформацією, поширення якої може порушувати законодавство України, а діяльність сайтів спрямована на підрив української державності, посягання на територіальну цілісність, суверенітет та незалежність України.

Зазначений Перелік долучено Прокуратурою АР Крим до матеріалів кримінального провадження за ознаками злочину, передбаченого ч.1 ст. 437 КК України за фактом вчинення невстановленими представниками Російської Федерації та підконтрольної їм окупаційної влади АР Крим протягом 2014-2017 років спланованої підготовки, розв’язування та ведення агресивної війни, зокрема активної інформаційної агресії за допомогою загальнодоступних та соціально-орієнтованих ресурсів мережі Інтернет,

спрямованої на дискредитацію України, як держави та формування потрібної РФ суспільної думки місцевого населення на тимчасово окупованій території півострова Крим.

3. Постійне поширення в інформаційному просторі маніпулятивної інформації, спрямованої на дискредитацію України на національному та міжнародному рівнях.

Службою безпеки України, Міністерством інформаційної політики України регулярно здійснюється моніторинг відкритих джерел інформації з подальшим реагуванням на потенційні ризики та загрози в інформаційній сфері. Зокрема:

розроблено та поширено серед центральних органів виконавчої влади довідковий матеріал щодо основних наративів російської пропаганди, що поширюються в інформаційному середовищі України, Росії та західних країн, станом на липень 2017-го року;

у межах інформаційного забезпечення судового процесу в Гаазі проти Росії – виявлено та розкрито ТОП-5 дезінформаційних меседжів російської сторони;

виявлено факти участі російської сторони у фінансуванні та підбурюванні провокаційних акцій з метою дестабілізувати і розхитати польсько-українські відносини, а також ведення подібної діяльності в Білорусі;

на протидію маніпулятивним заявам РФ, формується і поширюється офіційна позиція держави (яка, зокрема, ретранслюється іноземними ЗМІ) стосовно запровадження мовних квот та дотримання прав нацменшин, антиукраїнської риторики РФ щодо мовної політики в Україні та становища російської мови в Україні тощо [7].

4. Поширення видавничої продукції, що має походження або виготовлена та/або ввозиться з території держави-агресора, тимчасово окупованої території України, на митну територію України.

У 2017 році на книжковому ринку України з’явився такий важливий чинник, як дозвільна система щодо ввезення видавничої продукції, що має походження або виготовлена та/або ввозиться з території держави-агресора, тимчасово окупованої території України, на митну територію України.

Запроваджене обмеження імпорту російських книжок ще не вплинуло кардинально на ситуацію на вітчизняному книжковому ринку, однак створило додаткові умови для наповнення ринку книжками вітчизняних видавців .

Наразі українські імпортери отримують дозволи на ввезення книг з Росії. Починаючи з 18.05.2017 року надійшло на розгляд 4557 заяв про надання дозволу. Станом на 01.10.2017 року видано 4262 дозволів. Тираж видань, на які видано дозволи, становить 36 860 684 шт., заплановано реалізувати впродовж п’яти років.

Російські книжки у законний спосіб, відповідно до затвердженої дозвільної системи, потрапляють до України. Але їх кількість відчутно зменшується. Якщо минулого року в Україну було завезено близько 50 тис. назв російських книжок, то цього року йдеться про близько чотирьох тисяч. У грошовому виразі: якщо у 2013 році експорт з РФ становив 34,6 млн. дол. США, то в 2015 – лише 4,7 млн. дол. США.

Водночас надано відмови у видачі таких дозволів:

- близько 130 на підставі подання суб’єктом господарювання не в повному обсязі пакета документів, необхідних для одержання дозволу, або виявлення у поданих документах недостовірних відомостей;

- 14 відмов на підставі висновку експертної ради Держкомтелерадіо України у зв’язку з невідповідністю критеріям оцінки видавничої продукції, що дозволена до розповсюдження на території України. Наприклад, заборонено ввезення на територію України книжки одного із ідеологів російського фашизму Чапліна В.

“Православие.Честный разговор”, де пропагується “рускій мір”, розпалюється ненависть до інших народів [8].

Водночас, через обмеження ввезення російських книг в Україні дещо зменшилася кількість спеціалізованої наукової літератури. На сьогодні ця колишня російська ніша перекладної літератури заповнюється українськими книжками. Наразі спостерігається значне збільшення перекладних видань українською мовою. Українські видавці скуповують право перекладу українською мовою світових новинок і класики.

Головної мети – очищення українського книжкового ринку від видавничої продукції антиукраїнського змісту, Закон України “Про внесення змін до деяких законів України щодо обмеження доступу на український ринок іноземної друкованої продукції антиукраїнського змісту” [9] досяг. Запровадження дозвільної системи вплинуло на кількісну присутність продукції російських видавництв на ринку України і дало додатковий поштовх вітчизняному книговиданню, як на українській, так і на російській мовах.

Зазначений механізм жорстко контролює легальний ринок, але залишає поза увагою тіньовий. Кількість піратської продукції почала зростати. Це передусім малотиражна література, якої наразі бракує. Зокрема, нелегально завезені російські наукові видання за даними Держкомтелерадіо України зросли в ціні у півтора-два рази [8].

Висновки.

Як бачимо, ефективність діяльності державних органів у сфері захисту інформаційного простору України у 2017 році можливо визначати переважно за кількісними показниками. Окремі заходи мають поряд із безумовно позитивними деякі неоднозначні наслідки. Безумовно недоліками у сфері захисту національного інформаційної сфери на даний час є: недостатнє матеріально-технічне забезпечення протидії інформаційному впливу РФ; необхідність комплексного та системного впровадження та розвитку системи стратегічних (в т.ч. кризових) комунікацій, посилення міжвідомчої координації у сфері забезпечення інформаційної безпеки, в тому числі обміну інформацією, аналітикою та результатами моніторингу; існує нагальна потреба прийняття державою компенсаційних механізмів для вітчизняної книжкової торгівлі та бібліотек, що має на меті мінімізацію появи дефіциту книг на ринку тощо.

В цілому оцінити ефективність діяльності державних органів у сфері захисту національної інформаційної сфери за певний період не можливо шляхом виключно аналізу кількісних показників здійснених органами заходів неможливо. Критеріями оцінки такої діяльності має бути поінформованість українського суспільства і міжнародної спільноти про обґрунтованість, справедливість і доцільність здійснюваних заходів, а також, що найважливіше, сприйняття і підтримка українським суспільством і міжнародною спільнотою цілей, задля яких такі заходи здійснюються. Подібні індикатори можливо отримувати шляхом проведення соціологічних досліджень, на опрацювання методик яких спонукаємо представників соціологічної науки у співпраці з правниками-інформаційниками.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України” : Указ Президента України від 25.02.17 р. № 47/2017 // Офіційний вісник України. – 2017. – № 20. – С. 8.

2. Марущак А.І. Інформаційні ресурси держави : зміст та проблема захисту // Правова інформатика. – 2009. – № 1. – С. 64-70.

3. Про транскордонне телебачення : Європейська конвенція від 5 травня 1989 року // Офіційний вісник України. – 2010. – № 11. – С. 201.

4. Про внесення змін до деяких законів України щодо частки музичних творів державною мовою у програмах телерадіоорганізацій : Закон України від 16.06.16 р. // Відомості Верховної Ради України (ВВР). – 2016. – № 31. – Ст. 547.

5. Про телебачення і радіомовлення : Закон України від 21.12.93 р. // Режим доступу : http://zakon3.rada.gov.ua/laws/show/3759-12

6. Офіційний сайт Національної ради України з питань телебачення і радіомовлення. – Режим доступу : https://www.nrada.gov.ua.

7. Офіційний сайт Міністерства інформаційної політики України. – Режим доступу : mip.gov.ua.

8. Офіційний сайт Держкомтелерадіо України. – Режим доступу : http://comin.kmu.gov.ua.

9. Про внесення змін до деяких законів України щодо обмеження доступу на український ринок іноземної друкованої продукції антиукраїнського змісту : Закон України від 08.12.16 р. // Відомості Верховної Ради України (ВВР). – 2017. – № 4. – Ст. 41.

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

УДК 002.55:355.244.2

ЄРЕМЕНКО С.А., *кандидат технічних наук, доцент,*
заступник начальника Інституту державного управління
у сфері цивільного захисту з навчальної та методичної роботи

ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ АНАЛІТИЧНОЇ РОБОТИ У СФЕРІ ЦИВІЛЬНОГО ЗАХИСТУ

Анотація. *Статтю присвячено розгляду аналітичної роботи як необхідної умови об’єктивної оцінки ситуації щодо реалізації державної функції управління у сфері цивільного захисту в Україні. Розкрито роль аналітичної роботи в організації системи управління ризиками виникнення надзвичайних ситуацій.*

Ключові слова: *цивільний захист, державне управління, аналітична робота, управління ризиками виникнення надзвичайних ситуацій.*

Summary. *The article is devoted to the consideration of analytical work as a necessary condition for an objective assessment of the situation regarding the implementation of the state management function in the field of civil protection in Ukraine. The role of analytical work in the organization of the system of risk management of emergencies are examined.*

Keywords: *civil defence, state administration, analytical work, risk management of emergencies.*

Аннотация. *Статья посвящена рассмотрению аналитической работы как необходимого условия объективной оценки ситуации по реализации государственной функции управления в сфере гражданской защиты в Украине. Раскрыта роль аналитической работы в организации системы управления рисками возникновения чрезвычайных ситуаций.*

Ключевые слова: *гражданская защита, государственное управление, аналитическая работа, управление рисками возникновения чрезвычайных ситуаций.*

Постановка проблеми. Організації аналітичної роботи у сфері цивільного захисту приділяється постійна увага. Так, відповідно до Указу Президента України від 04 лютого 2003 року № 76/2003 “Про рішення Ради національної безпеки і оборони України від 11 листопада 2002 року “Про стан техногенної та природної безпеки в Україні” в країні щорічно, починаючи з 2003 року, здійснювалась підготовка і видання Національної доповіді про стан техногенної та природної безпеки в Україні. Відповідно до Указу Президента України від 06 червня 2014 року № 504/2014 “Про рішення РНБО України від 28 квітня 2014 року” (ч. 2 п. 4) вищезазначений Указ Президента України визнано таким, що втратив чинність [1].

Проте робота проведена для підготовки відповідної доповіді, дозволила побачити концептуальний напрям розвитку системи цивільного захисту, а саме Урядом було схвалено Концепцію управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру (далі – Концепція) [2].

В документі зазначено необхідність впровадження концептуальних засад управління ризиками виникнення надзвичайних ситуацій (далі – ризики), викликаних наявністю небезпечних чинників техногенного та природного характеру, зокрема:

- значною кількістю потенційно небезпечних об’єктів на території;
- високим рівнем травматизму та смертності населення, спричиненим небезпечними подіями і нещасними випадками;
- високим рівнем ризиків виникнення надзвичайних ситуацій природного характеру,

зумовленим глобальними та регіональними змінами клімату, зростанням сейсмічної активності тощо, а також інтенсифікацією впливу техногенної діяльності людини на навколишнє природне середовище;

- високим рівнем ризиків виникнення надзвичайних ситуацій техногенного характеру, зумовленим критичним ступенем зношеності (60 – 80 відсотків) основних виробничих фондів у галузях промисловості та агропромисловому комплексі;
- недостатнім технічним і технологічним рівнем розвитку державної системи спостережень за небезпечними чинниками, що зумовлюють виникнення надзвичайних ситуацій [2].

Ураховуючи світовий досвід, найбільш ефективним є управління ризиками, яке ґрунтується на досягненні певного рівня безпеки, балансу вигод і витрат в межах окремого об’єкта, території і держави в цілому.

Метою статті є оцінка ситуації щодо реалізації державної функції управління у сфері цивільного захисту в Україні.

Виклад основного матеріалу. На сьогодні механізми управління ризиками, спрямовані на зменшення їх значень, не набули широкого практичного застосування. Так, кількісна оцінка ризиків використовується лише в окремих областях, а саме під час аналізу безпеки атомних електричних станцій, декларування безпеки об’єктів підвищеної небезпеки. Разом з тим недосконалі нормативно-правові, організаційні та технічні методи управління ризиками не дають змоги сьогодні досягти рівнів ризиків, що відповідають рівням економічно розвинутих держав.

Метою зазначеної вище Концепції є запровадження сучасних методів управління ризиками для зменшення кількості та мінімізації соціально-економічних наслідків надзвичайних ситуацій, забезпечення досягнення гарантованого рівня безпеки громадянина і суспільства.

Концепція розрахована на довгострокову перспективу і є основою для розроблення нормативно-правових актів, загальнодержавних, регіональних та галузевих програм у сфері техногенної та природної безпеки.

Досягнення прийнятних рівнів ризиків на всій території України повинне здійснюватися поетапно.

На першому етапі необхідно визначити рівні ризиків для усіх галузей економіки, а також найбільш небезпечних джерел надзвичайних ситуацій та забезпечити їх зменшення до значень прийнятих рівнів ризику.

На другому етапі слід забезпечити досягнення рівнів ризиків на всій території України відповідно до рівнів, що використовуються в економічно розвинутих державах.

Наступним кроком у напрямі аналітичного забезпечення системи цивільного захисту в Україні стало Розпорядження Кабінету Міністрів України від 25 березня 2015 р. № 419-р. [3], яким затверджено “План заходів щодо реалізації Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру на 2015 – 2020 роки”. В Плані заходів передбачено проведення аналізу стану техногенної та природної безпеки в Україні та на основі отриманих результатів здійснення районування території України з урахуванням наявних потенційно небезпечних об’єктів, ризиків виникнення небезпечних геологічних, гідрогеологічних та метеорологічних явищ і процесів. УкрНДІЦЗ у співпраці з центральними та місцевими органами виконавчої влади, науковими закладами, заінтересованими установами та організаціями було проведено аналіз стану техногенної та природної безпеки в Україні за 2015 рік, результатом якого став аналітичний огляд.

Відповідний документ було спрямовано на всебічний аналіз наявної інформації про стан техногенної та природної безпеки, функціонування Єдиної державної системи цивільного захисту під час ліквідування наслідків надзвичайних ситуацій (далі – НС), на окреслення основних існуючих проблем у сфері техногенної і природної безпеки в Україні та визначення шляхів і способів їх розв’язання, на удосконалення системи попередження і реагування на НС техногенного та природного характеру. Крім того, в Аналітичному огляді наведено результати прогнозування виникнення НС, що дає змогу завчасно провести запобіжні заходи, знизити ризики виникнення та зменшити збитки від наслідків НС.

Положення Концепції знаходять свою реалізацію в проектах нормативно-правових актів. Так, на офіційному сайті Державної служби України з надзвичайних ситуацій (//www.dsns.gov.ua) розміщено проект наказу МВС України “Про затвердження Положення про організацію управління ризиками” [4]. Метою проекту наказу є забезпечення організації процесів управління ризиками в різних галузях економіки. Зазначається, що реалізація проекту наказу дозволить організувати процеси з управління ризиками виникнення надзвичайних ситуацій та запровадити сучасні методи управління безпекою у галузях економіки, спрямовані на збалансоване вирішення соціально-економічних завдань, проблемних питань пожежної, техногенної безпеки та цивільного захисту, збереження сприятливого стану навколишнього природного середовища [5]

З вищевикладеного стає зрозумілим, що державне управління у сфері цивільного захисту – це цілеспрямована діяльність, для ефективної реалізації якої потрібен механізм опрацювання величезного обсягу інформації, необхідної для визначення завдань на близьку, середню та далеку перспективу, визначення порядку збирання, систематизації та оцінки інформації, механізм її руху по вертикалі та горизонталі управління, порядок обміну інформацією як на національному, так і міжнародному рівнях, повноваження керівного складу та аналітичних підрозділів.

Таким чином, ми підходимо до необхідності застосовувати цілісну систему, яка дозволяє отримувати знання про об’єкт управління відповідно до поставлених цілей. Таким інструментарієм в процесі реалізації державної політики у сфері цивільного захисту є моніторинг.

Термін “моніторинг” має англійське походження, і в дослівному перекладі означає monitoring (від лат. monitor) – спостережний. Вперше термін “моніторинг” використано на Стокгольмській конференції Організації Об’єднаних Націй з проблем довкілля, яка проводилась 5 – 16 червня 1972 р. Саме тоді було запроваджено систему моніторингу навколишнього середовища. Перші пропозиції з приводу такої системи було розроблено експертами спеціальної комісії SCOPE Наукового комітету з проблем довкілля в 1979 р. Систему повторних досліджень однієї та більшої кількості подій чи явищ, у просторі та часі, з визначеною метою і відповідно до підготовленої програми, було запропоновано назвати моніторингом.

Згодом цей термін став не лише новим означенням вже давно існуючих аналітичних і прогнозуючих принципів, а набув чіткого визначення системності та методики його проведення. Системи моніторингу, модельовані відповідно до галузевої специфіки, використовуються не лише в екології, але і в медицині, геології, соціології та в практиці космічних наук.

Наразі у словниках іншомовних слів, у фінансово-економічних та енциклопедичних словниках визначення терміна “моніторинг” практично однакове, а якщо й існують відмінності, то лише з урахуванням сфери його застосування. Межі використання моніторингу за останнє десятиліття надзвичайно розширились.

Моніторинг може розглядатися як спосіб дослідження реальності, що використовується в різних науках, і як спосіб забезпечення сфери управління різними видами діяльності шляхом подання своєчасної та якісної інформації.

Таким чином, моніторинг є важливою складовою процесу управління складною системою, ефективне здійснення якого залежить від способів дослідження реальності в якості об’єкта впливу.

Відповідно до Кодексу цивільного захисту України такою системою виступає Єдина державна система цивільного захисту [6]. Статтею 8 зазначеного Кодексу визначено, що Єдина державна система цивільного захисту забезпечує реалізацію державної політики у сфері цивільного захисту, здійснюється Єдиною державною системою цивільного захисту, яка складається з функціональних і територіальних підсистем та їх ланок. Процес реалізації державної політики неможливо організувати та реалізовувати без налагодженої системи отримання інформації про об’єкт управлінського впливу, про стан захисту населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій, про запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період.

Саме моніторинг виступає ключовим елементом у формуванні та реалізації державної політики у сфері цивільного захисту, необхідним елементом організації Єдиної державної системи цивільного захисту. На чому він повинен базуватись, знаходити підґрунтя для дослідження об’єктивної реальності, таку основу надає національна безпека. В частині першій ст. 6 “Суб’єкти забезпечення цивільного захисту” Кодексу визначено, що цивільний захист забезпечується з урахуванням особливостей, визначених Законом України “Про основи національної безпеки України”, суб’єктами, уповноваженими захищати населення, території, навколишнє природне середовище і майно, згідно з вимогами цього Кодексу – у мирний час, а також в особливий період – у межах реалізації заходів держави щодо оборони України [6].

Виходячи з цього, цивільний захист в аспекті функціонування в системі національної безпеки полягає у реалізації управлінського впливу через призму захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам:

- невідповідність сучасним викликам стану Єдиної державної системи цивільного захисту, сил цивільного захисту, їх технічного оснащення;
- значне антропогенне і техногенне перевантаження території України, зростання ризиків виникнення надзвичайних ситуацій техногенного та природного характеру;
- погіршення технічного стану гідротехнічних споруд каскаду водосховищ на річці Дніпро;
- непідтримання в належному технічному стані ядерних об’єктів на території України;
- небезпека техногенного, у тому числі ядерного та біологічного, тероризму (ст. 7 Закону України “Про основи національної безпеки України”) [7].

Для організації повноцінного процесу управління керуючому органу необхідна інформація про загрози та про те, як у прямій залежності від загроз у певній сфері суспільного життя визначаються напрями державної політики з питань національної безпеки у сфері цивільного захисту:

- забезпечення ефективного функціонування Єдиної державної системи цивільного захисту, оснащення сучасними видами техніки сил цивільного захисту;

- вжиття організаційних, економічних, інженерно-технічних та інших заходів для зниження ризиків виникнення надзвичайних ситуацій до прийнятних рівнів;
- підвищення рівнів екологічної, ядерної та радіаційної безпеки до норм і стандартів у відповідній сфері, в тому числі перетворення об’єкта “Укриття” Чорнобильської АЕС на екологічно безпечну систему (ст. 8 Закону України “Про основи національної безпеки України”) [7].

Процес управління системою національної безпеки передбачає отримання повноцінної інформації про загрози у певній сфері та на основі її опрацювання прийняття управлінських рішень, однією з формою яких є державна політика.

Із зазначеного випливає, що питання цивільного захисту є одним з напрямів моніторингу у сфері національної безпеки. Для Єдиної державної системи цивільного захисту результатом його проведення є державна політика, яка формується та реалізується у рамках національної безпеки і виконується суб’єктами цієї системи. Здійснення моніторингу на рівні національної безпеки має нормативно-правове підґрунтя, і його здійснення є однією з функцій уповноважених суб’єктів забезпечення національної безпеки.

Наступний рівень моніторингу у сфері цивільного захисту визначається необхідністю реалізації функції держави, яка спрямована на захист населення, територій, навколишнього природного середовища та майна від надзвичайних ситуацій шляхом запобігання таким ситуаціям, ліквідації їх наслідків і надання допомоги постраждалим у мирний час та в особливий період. Для організації цього виду моніторингу необхідно використовувати положення Кодексу цивільного захисту України. Ключовим елементом пізнання об’єктивної реальності виступає надзвичайна ситуація. Її визначення наведене в п. 24 ст. 2 “Визначення термінів”. Надзвичайна ситуація – обстановка на окремій території чи суб’єкті господарювання на ній або водному об’єкті, яка характеризується порушенням нормальних умов життєдіяльності населення, спричинена катастрофою, аварією, пожежею, стихійним лихом, епідемією, епізоотією, епіфітотією, застосуванням засобів ураження або іншою небезпечною подією, що призвела (може призвести) до виникнення загрози життю або здоров’ю населення, великої кількості загиблих і постраждалих, завдання значних матеріальних збитків, а також до неможливості проживання населення на такій території чи об’єкті, провадження на ній господарської діяльності;

Статтею 5 “Класифікація надзвичайних ситуацій” Кодексу цивільного захисту України передбачено:

1. Надзвичайні ситуації класифікуються за характером походження, ступенем поширення, розміром людських втрат та матеріальних збитків.

2. Залежно від характеру походження подій, що можуть зумовити виникнення надзвичайних ситуацій на території України, визначаються такі види надзвичайних ситуацій:

1) техногенного характеру;

2) природного характеру;

3) соціальні;

4) воєнні.

3. Залежно від обсягів заподіяних надзвичайною ситуацією наслідків, обсягів технічних і матеріальних ресурсів, необхідних для їх ліквідації, визначаються такі рівні надзвичайних ситуацій:

1) державний;

2) регіональний;

3) місцевий;

4) об’єктовий.

4. Порядок класифікації надзвичайних ситуацій за їх рівнями встановлюється Кабінетом Міністрів України [6].

Підпунктом 5 ст. 5 класифікаційні ознаки надзвичайних ситуацій визначаються центральним органом виконавчої влади, який забезпечує формування та реалізує державну політику у сфері цивільного захисту.

Висновки.

Закріплена на законодавчому рівні класифікація надзвичайних ситуацій свідчить про те, що проведено ґрунтовну науково-дослідну роботу щодо узагальнення досвіду протидії небезпечним факторам, які мають місце у різних сферах суспільного життя.

Разом з тим суб’єкту управління у сфері цивільного захисту необхідно отримувати інформацію про реальний стан змін в об’єктивній реальності внаслідок надзвичайних ситуацій. Це обумовлено тим, що ефективність системи цивільного захисту залежить від можливостей відповідних суб’єктів прогнозувати варіанти розвитку ситуацій на основі моніторингу взаємопов’язаних подій, що характеризує стан безпеки у певній сфері суспільного життя.

Таким чином, моніторинг реалізації державної політики у сфері цивільного захисту повинен здійснюватись на рівні суб’єктів забезпечення національної безпеки та Єдиної системи цивільного захисту, з урахуванням особливостей організації процесу управління як системи в цілому, так і окремих її елементів.

Використана література

1. Про рішення Ради національної безпеки і оборони України від 11 листопада 2002 року “Про стан техногенної та природної безпеки в Україні” : Указ Президента України від 04.02.03 р. № 76/2003. – (Указ втратив чинність на підставі Указу Президента від 06.06.14 р. № 504/2014). – Режим доступу : http://zakon0.rada.gov.ua/laws/show/76/2003

2. Про схвалення Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру : Розпорядження Кабінету Міністрів України від 22.01.14 р. № 37-р. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/37-2014-р

3. Про затвердження плану заходів щодо реалізації Концепції управління ризиками виникнення надзвичайних ситуацій техногенного та природного характеру на 2015 – 2020 роки : Розпорядження Кабінету Міністрів України від 25.03.15 р. № 419-р. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/419-2015-р

4. Офіційний сайт Державної служби надзвичайних ситуацій. – Режим доступу : www.dsns.gov.ua

5. План заходів Державної служби України з надзвичайних ситуацій на 2018 рік щодо реалізації Національної стратегії сприяння розвитку громадянського суспільства на 2016 – 2020 роки. – Режим доступу : http://www.dsns.gov.ua/ua/Elektronni-konsultaciyi-z-gromadskistyu.html

6. Кодекс цивільного захисту України : Закон України від 28.12.14 р. № 76-VIII (редакція від 12.05.17 р.). – Режим доступу : http://zakon2.rada.gov.ua/laws/show/5403-17

7. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV (редакція від 09.07.17 р.). – Режим доступу : http://zakon2.rada.gov.ua/laws/show/964-15

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

УДК 004.056.53

УХАНОВА Н.С., старший науковий співробітник
НДІ інформатики і права НАПрН України

ЗАХИСТ ІНФОРМАЦІЙНОГО ПРОСТОРУ ВІД ТЕРОРИСТИЧНИХ ПОСЯГАНЬ ТА НЕГАТИВНИХ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИХ ВПЛИВІВ

***Анотація**. В статті розглядаються інформаційно-психологічні та суспільно-правові аспекти використання сучасного інформаційного простору та інформаційно-комунікаційних технологій на шкоду людині, суспільству і державі. Розкрито питання терористичних викликів і загроз з використанням інформаційного простору. Проаналізовано інформаційно-психологічні механізми здійснення інформаційних операцій, маніпулювання, ідеологічного впливу і вербування прибічників терористичних та інших злочинних організацій з використанням інформаційно-комунікаційних технологій.*

***Ключові слова**: інформаційний простір, інформаційно-комунікаційні технології, інформаційно-психологічний вплив, інформаційний тероризм, кібератаки, маніпуляція.*

***Summary.** The article considers informational and psychological, as well as public and legal aspects of the use of modern information space and information and communication technologies to the damage of human, society and state. The issue of terrorist challenges and threats with the use of information space is explored. The informational and psychological mechanisms of implementation of information operations, manipulation, ideological influencing and recruiting of supporters of terrorist and other criminal organizations with the use of information and communication technologies are analysed.*

***Keywords:** information space, information and communication technologies, information and psychological influencing, information terrorism, cyber attacks, manipulation.*

***Аннотация**. В статье рассматриваются информационно-психологические и общественно-правовые аспекты использования современного информационного пространства и информационно-коммуникационных технологий во вред человеку, обществу и государству. Раскрыт вопрос террористических вызовов и угроз с использованием информационного пространства. Проанализированы информационно-психологические механизмы осуществления информационных операций, манипулирования, идеологического влияния и вербовки сторонников террористических и других преступных организаций с использованием информационно-коммуникационных технологий.*

***Ключевые слова:** информационное пространство, информационно-коммуникационные технологии, информационно-психологическое влияние, информационный терроризм, кибератаки, манипуляция.*

Постановка проблеми. Сучасний світ уже давно вступив в епоху глобалізації, яка безпосередньо позначається на усіх сферах життєдіяльності людини, суспільства і держави. Під її впливом трансформуються і активно розвиваються інформаційні технології, інформаційні ресурси, продукти і послуги, а сама інформація стала могутньою зброєю для широкого застосування.

Водночас, за нашими оцінками, правове регулювання інформаційних відносин суттєво відстає від техніко-технологічного розвитку інформаційної сфери, що “de facto” розбудовується в Україні протягом останніх 15 – 20 років. При цьому, глобальна інформаційна інфраструктура та її базові компоненти, як об’єкти правового регулювання, та проблеми транскордонного використання інформаційно-комп’ютерних технологій знаходяться на початковому етапі дослідження. Зазначене, власне, і визначає актуальність звернення до обраної теми.

Результати аналізу наукових публікацій. Системний аналіз правових аспектів використання віртуальних технологій почався в зарубіжній правовій доктрині у 90-х рр. минулого століття, а віртуальні технології досліджувалися як технологічний ресурс і як загальнонаукове ключове поняття та феномен, який впливає на соціальний контекст правового регулювання. Як свідчить аналіз наукових здобутків, найбільший науковий і практичний інтерес представляють фундаментальні дослідження Л. Лесссіга (Lessig L.) з проблематики нормативно-технічних і правових засобів регулювання кіберпростору, “нормативної мінливості” регулювання, об’єктивно обумовленої розвитком програмно-технологічного забезпечення; роботи В. Майера-Шонбергера (Mayer-Schqnberger V.) і М. Цівіца (Ziewitz M.), присвячені питанням неминучості правового регулювання транскордонного використання інформаціфних технологій засобами міжнародного права; роботи Дж. Голдсміта (Goldsmith J.) і Т. Ву (Wu T.) і їх фундаментальне дослідження, що узагальнило 20-річну еволюцію регулювання технологій в роботі “Хто контролює Інтернет: ілюзії безмежного світу” (2006 р).

Метою статті є висвітлення актуальних питань використання інформаційних технологій та інформаційного простору як інформаційної зброї, характеру впливу Інтернет-ресурсів на масову свідомість та відповідних правових аспектів у цій сфері.

Виклад основного матеріалу. Динамічне поєднання і взаємодія нових інформаційних технологій та засобів зв’язку поклали початок виникненню нового феномену, який отримав назву “інформаційний простір” (за окремими джерелами – “кіберпростір”). Це середовище електромагнітних процесів, обробки цифрових даних та їх передачі, приховане від візуального сприйняття, проте воно є вкрай важливим для стану економіки і добробуту суспільства.

Стосовно понятійно-категоріального апарату варто звернути увагу, що одним із базових в інформаційній сфері є поняття “інформаційний простір”, яке також одержало відповідне наукове визначення. Водночас, у низці досліджень і документів застосовується й дещо інший термін – “віртуальний простір”. Зокрема, на думку Л. Лесссіга, *віртуальний простір – це технічна конструкція, що базується на зведенні норм і правил, які обумовлюють формат регулювання віртуальних технологій*. При цьому, в якості норм і правил, тобто “кодексу”, або “коду” (Code), виступає програмне забезпечення, віртуальна архітектура, протоколи і стандарти Інтернету. Саме цей “звід норм” слід розглядати як нормативний “кодекс”, здатний регулювати і накладати обмеження на поведінку учасників, і який може забезпечити можливості для досить широкого контролю, оскільки технічна архітектура віртуального простору регулює свободу особистості таким же чином, яким право і правові норми регулюють суспільні відносини [1].

Основний принциповий висновок, до якого приходять Д. Голдсміт і Т. Ву стосовно правових аспектів використання інформаційно-комп’ютерних технологій полягає в тому, що всі наші припущення щодо майбутнього Інтернету були невірні, оскільки територіальне регулювання можливо і насправді затребуване, а Інтернет слід розглядати як “віртуальний простір”, в якому територіальне право, державна влада та міжнародні відносини відіграють таку ж роль, як і технологічні винаходи [2, с. 118].

Як зазначає Е. Лонгворт, інше поняття – “кіберпростір” слід розглядати як “міжнародний простір”, подібний до міжнародних вод Антарктиди, стосовно якого слід використовувати ті ж само правові регулятивні механізми [3, с. 24]. Тобто, сфера регулювання транскордонного використання інформаційно-комп’ютерних технологій пов’язана з комплексом завдань і проблем, вирішення яких лежить у площині міжнародного права.

Загалом, у нормотворчій практиці більш усталеним є використання поняття *“інформаційний простір”*, а стосовно інформаційно-комп’ютерних технологій та програмних продуктів – *“кіберпростір”*. Термін *“віртуальний простір”* переважно розглядається як синонімічний. Також слід звернути увагу на низку актуальних аспектів:

по-перше, питання полягає не в тому, чи можна застосовувати міжнародне право до “інформаційного простору” або “кіберпростору”, оскільки позитивна відповідь на це питання не викликає сумнівів, а в тому, які саме форми і методи при цьому мають використовуватись;

по-друге, рамки застосування міжнародного права не слід зводити до системи обмежень, що накладаються чинним міжнародним правом на національні або регіональні підходи у сфері регулювання застосування інформаційно-комп’ютерних технологій;

по-третє, міжнародне право може бути застосоване до Інтернету, а Інтернет впливає на міжнародне право. При цьому, теза про виникнення нового міжнародного права, про що йшлося в окремих працях західної правової доктрини, є дискусійною;

по-четверте, існуюча реальність не підтвердила припущень про те, що регулювання відносин у сфері Інтернету настільки різноманітне і “породжує такі синергетичні зв’язки”, які можуть трансформувати роль суверенних держав як суб’єктів міжнародного права.

У той же час, великі перспективи, що відкривають перед людством новітні технології, та зростаюча залежність від них пов’язані з низкою проблем, на які необхідно звернути увагу. Однією з таких проблем є протиправні дії в інформаційній сфері, у тому числі кібератаки, кібертероризм, комп’ютерне шпигунство та використання шкідливого програмного забезпечення для перешкоджання вкрай важливим процесам життєдіяльності суспільства.

Сьогодні інформаційно-комп’ютерні технології перестали бути якимось “єдиним” об’єктом регулювання, оскільки являють собою багаторівневу мережу, глобальна технологічна інфраструктура якої забезпечує їх транскордонне функціонування і використання, що підлягає врахуванню при правовому регулюванні відносин у досліджуваній сфері. Технологічно складна глобальна багаторівнева структура інформаційних технологій охоплює кілька інфраструктурних рівнів, починаючи від “найнижчого” – “фізичного” рівня (канали зв’язку волоконно-оптичних ліній, супутникові канали, радіочастотний спектр та ін.), закінчуючи “вищим” рівнем Інтернет-додатків (веб портали і сайти, соціальні мережі, поштові сервіси тощо). На кожному з інфраструктурних рівнів інформаційних технологій складаються стосунки, які виникають з приводу різних і досить специфічних об’єктів регулювання. При цьому, такі компоненти багаторівневої глобальної технологічної інфраструктури, як номерні ресурси адресації (глобальний пул IP-адресного простору, номери автономних систем, портів і протоколів і т.ін.), система доменних імен верхнього рівня, кореневі сервери системи доменних імен, є базовими (фундаментальними) і обумовлюють транскордонне функціонування і використання інформаційних технологій.

Протягом першого десятиліття XXI ст. у процесі правового регулювання пріоритетна увага приділялася кібератакам та інформаційним війнам. Але не так давно колишній співробітник Агентства національної безпеки США Едвард Сноуден розголосив відомості, що становлять державну таємницю, та розкрив більше інформації, ніж найкращий розвідник зміг би зібрати за часів холодної війни. Не слід забувати, що Сноуден навіть не був суперагентом – просто завдяки сучасним технологіям він мав

доступ до великого масиву даних, які в минулому отримати було б просто неможливо. У зв’язку з цим слушним видається питання: як у майбутньому забезпечити ефективний захист даних від несанкціонованого доступу? Нині ми більш повно маємо усвідомлювати необхідність захисту інформації.

Як відомо, норми міжнародного права і національні законодавства надають право національним спецслужбам здійснювати технічну розвідку та збирати за її допомогою інформацію стратегічного, оперативного чи тактичного рівня. На прикладі Сноудена варто звернути увагу на особливості технічної розвідки США (наприклад, на програму спостереження “ПРИЗМА”). Ця специфіка обумовлена тим, що такого роду діяльність реалізується з опорою на закони, які дозволяють зберігати і фільтрувати дані в технічно можливому обсязі. За необхідності – наприклад, в рамках боротьби з тероризмом – американські розвідувальні служби можуть збирати інформацію всередині країни і за кордоном. На території США на заходи зі збору відомостей поширюються положення американського законодавства, і при цьому США, керуючись зрозумілою логікою, використовують всі доступні їм нормативні та технічні засоби. Але, якщо мова йде про інформаційний простір, то в цій сфері загальновизнаних правил поки що не існує.

Однією з найбільш актуальних нині проблем інформаційного простору або кіберпростору є проблема запобігання і протидії кібератакам, що здійснюються в результаті проникнення чи зламу комп’ютерних програм і систем, апаратних засобів, засобів цифрового захисту тощо. Україна в умовах гібридної війни протягом тривалого часу є пріоритетною мішенню для кібератак та здійснення негативного інформаційно-психологічних впливу на шкоду людині і суспільству у національному інформаційному просторі з боку РФ та злочинних організацій. Для проведення кібератак використовуються не лише такі засоби, як програми “троянський кінь” або заражені вірусом електронні повідомлення. Тепер удари наносяться з максимальною точністю в ході “соціально-технічних нападів” з використанням вірусів спеціалізованих різновидів. При цьому атакуючий суб’єкт завчасно вивчає, хто в організаційній структурі чи системі електронного управління займає важливу позицію та хто відкриє і прочитає електронне повідомлення з певним адресним рядком.

В сучасному світі також поширюється використання інформаційного простору терористичними, сепаратистськими та екстремістськими організаціями і групами. Вони використовують цей простір для агітації, пропаганди своїх поглядів і вербування поплічників, провокації масових безладів, диверсій тощо. При цьому радикалізація стосується перш за все процесу ідеологічної обробки, який нерідко супроводжує перетворення завербованих неофітів на осіб, сповнених рішучості здійснювати насильницькі дії на основі екстремістських ідеологій. Процес радикалізації часто включає використання пропаганди, яка протягом тривалого часу ведеться або за допомогою особистого спілкування, або через Інтернет. Зазначимо, що тривалість і ефективність пропаганди та інших використовуваних засобів переконання варіюється залежно від конкретних обставин і відносин.

Свобода в інформаційному просторі робить можливим широке застосування інформаційно-психологічних технологій формування громадської думки і нав’язування людині тих чи інших міфологічних уявлень або заданих стереотипів поведінки і мислення. Маніпуляція орієнтована на елімінацію логіки, критичного аналізу і примітивізацію мислення цільової групи, підміну логічного стійкого асоціативного зв’язку, коли те чи інше явище асоціюється з деструктивним образом, що нав’язується. У цьому аспекті самостійний погляд на світ, спроби незалежного мислення на основі здорового глузду, а не в рамках нав’язуваної міфологічної парадигми, міфологічного

образу світу і вкорінених у ньому стереотипів поведінки і цінностей представляє основну небезпеку для будь-якої маніпуляційної програми.

Елементами маніпуляційної програми є міфи, в тому числі міфи про рішення долі і т.ін., що вселяє думку про покірність і безглуздість критичного аналізу існуючого порядку речей. Однак вразливим місцем будь-якої маніпуляції є альтернативні джерела інформації, альтернативний погляд, вміння критично аналізувати запропонований варіант вирішення проблеми. Умовою ефективності маніпуляції є виведення масової свідомості за звичні рамки норм, цінностей і стереотипів, дестабілізація масової свідомості за допомогою пропагандистських і відволікаючих заходів. Ступінь ефективності маніпулювання залежить від глибини і точності сканування ментальних структур групи: її норм, цінностей, стереотипів.

Наприклад, ІДІЛ можна порівняти з дуже потужною сектою. Спочатку з об’єктом вербування знайомиться людина, чоловік або жінка. Робиться це через інтернет: соціальні мережі, месенджери, сайти знайомств, спільноти, форуми і так далі. Все це на тлі дезінформації в мережі у вигляді новинних джерел. Починається спілкування та підбирається ключ до особистості. Легше працювати з людьми вразливими, з тонкою душевною організацією, невпевненими в собі, які не мають своєї особистої думки чи зі спотвореним уявленням про світ. Це – люди без “стрижня” [**Ошибка! Источник ссылки не найден.**, с. 456].

Як бачимо, характерна особливість людського сприйняття полягає в тому, що людина краще засвоює ту інформацію, яка схожа на вже існуючі у неї уявлення. Основні засоби інформаційної війни орієнтовані на цю особливість. Будь-які маніпуляції та пропагандистські компанії засновані на “ефекті резонансу”, коли інформація, що “імплантується”, спрямована на зміну поведінки спільності, маскуються під знання і стереотипи, вже існуючі в конкретній соціальній спільності, на яку спрямована пропагандистська компанія. Розвиток засобів і технологій інформаційної війни робить дедалі більш актуальними розробку засобів протидії маніпулятивним технологіям, а також розвиток методів управління і захисту інформаційного простору, заснованих на демократичних нормах свободи слова. Тому, незабаром, виявляється, що цей новий знайомий має багато схожих інтересів, аналогічне хобі, захоплення, погляд на життя.

Після довгого листування один пропонує модель іншого суспільства з аналогічними можливостями і псевдоцінностями. Головне – закласти фундамент. Вибір людини і закладка фундаменту – це перший етап. Далі “мотиватор” формує уявлення про те, що є несправедливості, що “жертва” може і повинна знайти своє місце в житті. Реалізувати плани. Внести особистий внесок. Адже кожен хоче бути корисним, необхідним. Потрібно зробити щось важливе. Промивання мізків відбувається повільно і поступово.

В останні роки терористичні організації все частіше вдаються до використання Інтернету в якості альтернативної бази для підготовки терористів. Дедалі ширший спектр засобів інформації надає платформи для поширення практичних посібників у вигляді інтерактивних навчальних посібників, аудіо- та відеокліпів, інформаційних повідомлень і рекомендацій. На цих Інтернет-платформах також публікуються докладні інструкції, часто в легкодоступному мультимедійному форматі і на декількох мовах, з таких питань, наприклад, як вступити до терористичних організацій, як виготовити вибухові боєприпаси, вогнепальну та інші види зброї або небезпечні матеріали і як планувати і здійснювати терористичні акти. Ці платформи виступають в якості навчальної бази. Крім того, вони використовуються, зокрема, для обміну спеціальними методами, прийомами та сучасними знаннями з метою вчинення терористичних актів.

У наявних в Інтернеті навчальних матеріалах пропонуються інструменти для протидії або захисту від оперативно-розшукової та розвідувальної діяльності, неавторизованого доступу до комп'ютерних даних, а також для підвищення рівня захищеності протизаконних комунікацій і діяльності у інформаційно просторі шляхом використання доступних засобів шифрування і методів анонімізації. Інтерактивний характер інтернет-платформ допомагає створити відчуття спільності між людьми, що живуть в різних географічних регіонах і мають різне походження, сприяючи створенню мереж для обміну матеріалами навчального і тактичного характеру. Терористичні мережі часто характеризуються як “клітинні” – створені з майже незалежних клітинок. Формальне визначення “літинних мереж” було надане у термінах мережевих компонентів і властивостей. Клітинні мережі мають такі властивості, як надмірність, наявність тісно зв‘язаних клітинок (4 – 6 осіб), відсутність управління вертикальним способом (нечіткі директиви), відсутність планування (формування за рахунок локальних обмежень), можливість еволюціонування у відповідь на деструктивну діяльність [5, с. 111].

Відзначимо, що інформаційні війни спрямовані не тільки проти держави і найважливіших об’єктів її інфраструктури, але і проти екстремістів-опонентів. У більшості випадків потенціал скоєних кібератак та інформаційних операцій обмежений у зв’язку з дефіцитом знань. Це позбавляє їх організаторів можливості здійснювати великомасштабні напади. Але досягнувши необхідного професійного рівня, екстремісти зможуть завдавати більшої шкоди.

Чинна міжнародно-правова база у сфері боротьби з тероризмом міститься в різних джерелах, включаючи резолюції Генеральної Асамблеї та Ради Безпеки ООН, договори, судову практику і міжнародне звичаєве право. Резолюції Ради Безпеки можуть накладати на держави-члени юридично зв’язуючі та політичні зобов’язання, що належать до сфери т.зв. “м’якого права”, або сприяти формуванню нових міжнародно-правових норм. Резолюції Ради є обов’язковими для всіх держав-членів. Генеральна Асамблея також прийняла ряд резолюцій про боротьбу з тероризмом, які є корисними джерелами “м’якого права” та мають велике політичне значення, хоча і не є юридично обов’язковими. Юридичні зобов’язання також накладаються на держави відповідно до двосторонніх і багатосторонніх документів щодо боротьби з тероризмом. Обов’язок притягати винних у скоєнні терористичних актів до судової відповідальності лягає, насамперед, на внутрішньодержавні органи влади, оскільки міжнародні суди, як правило, не мають юрисдикції щодо таких актів.

Висновки.

В цілому, розгляд сучасних викликів і загроз, пов’язаних із розвитком інформаційно-комп’ютерних технологій та інформаційного простору або кіберпростору, а також питань захисту інформаційного простору від терористичних посягань та негативних інформаційно-психологічних впливів підсумуємо низкою висновків та пропозицій, зокрема:

1. У XXI столітті захист даних та безперебійне функціонування інформаційно-комунікаційних систем і систем зв’язку значною мірою впливають на усі сфери життєдіяльності людини, суспільства і держави. В інформаційному просторі формуються новітні виклики і загрози щодо захисту даних, комп’ютерних систем і мереж та приватного життя громадян. Все більшого поширення набувають факти здійснення інформаційно-психологічних операцій на шкоду людині та суспільству, які також створюють реальні загрози державному суверенітету і територіальній цілісності

держав. Динаміка трансформації сучасних викликів і загроз не відстає від темпів розвитку інформаційно-комп’ютерних технологій та інформаційного простору.

2. Сучасну інформаційну війну, як одну із основних складових гібридної війни, за нашими оцінками, варто розглядати як боротьбу за цілком реальну владу, спробу глобального перерозподілу сфер впливу та розшарування суспільств і країн-членів ЄС і НАТО. Застосування інформаційної зброї, у т.ч. кібератак, відбувається за різними векторами екстремістського спектру *(наприклад, “партизанські” напади в кіберпросторі лівих екстремістів, заклики до створення “інституту віртуального джихаду” тощо)*. При цьому життєво необхідно запобігти можливому нанесенню кібератак на системи контролю даних і нападів з метою заволодіння контролем за системами електронного (цифрового) управління об’єктами критичної інфраструктури *(електро-, водо- і газопостачання, авіаційного і залізничного руху, біржовою і банківською діяльністю тощо)*.

3. Використання інформаційного простору (кіберпростору) в терористичних та інших злочинних цілях стало суттєвою транснаціональною проблемою. Для її вирішення потрібні узгоджені заходи транскордонного характеру за участі міжнародних і національних правоохоронних систем та систем безпеки. Значна роль у зв’язку з цим має приділятися комплексу двосторонніх і багатосторонніх заходів та обміну досвідом між державами, а також досягненню консенсусу щодо питань боротьби з тероризмом та іншими злочинами в інформаційній сфері. Також актуалізується проблема розвитку міжнародної, регіональних і національних систем інформаційної безпеки та потреба підвищення ефективності міжнародного співробітництва національних спецслужб і правоохоронних органів у цій сфері.

Використана література

1. Lessig L. Code and other Laws of Cyberspace. – Режим доступу : http://www.archiv.orgc yber.law.harvard.edu/lessigbio

2. Goldsmith J. and Wu T. Who Controls the Internet? : Illusions of a Borderless World. – New York : Oxford University Press, 2006. – 219 p.

3. Longworth E. Possibilities of a Legal Framework for Cyberspace: Including a New Zealand Perspective. Prepared for the Unesco Experts Meetings on Cyberspace Law. 2010. – Pp. 23-29.

4. Lipton Jacqueline D. Bad Faith in Cyberspace : Grounding Domain Name Theory in Trademark, Property, and Restitution. Harvard Journal of Law & Technology. Volume 23. Number 2 Spring 2010. – P. 451-457.

5. Ланде Д.В. Основи інформаційного та соціально-правового моделювання : навч. посіб. / Д.В. Ланде , В.М. Фурашев , К.В. Юдкова. – К. : НТУУ “КПІ”, 2014. – 220 с.

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

Інформація в інших галузях права

УДК 004.8:343.22+343.412

РАДУТНИЙ О.Е., *доктор філософії (Ph.D.) з юридичних наук, доцент*,
доцент кафедри кримінального права № 1
Національного юридичного університету ім. Ярослава Мудрого

ШТУЧНИЙ ІНТЕЛЕКТ ЯК СУБ’ЄКТ ЗЛОЧИНУ

***Анотація**: В статті досліджуються питання про можливість визнання штучного інтелекту (електронної особи) суб’єктом кримінально-правових відносин та суб’єктом злочину, потенційних інформаційних та інших загроз з боку штучного інтелекту, можливість збереження контролю на останнім, зв’язок інформаційної безпеки з дослідженнями штучного інтелекту та їх результатами.*

***Ключові слова**: штучний інтелект, об’єкт робототехніки, суб’єкт злочину, електронна особа, заходи кримінально-правового характеру щодо електронних осіб, криптовалюта, Великі Дані.*

***Summary:** The article deals with the possibility of recognition for the artificial intelligence (electronic person) as a subject of criminal and legal relations and as a subject of a crime, potential information and other threats on the part of the artificial intelligence, maintaining control over it, link between information security and studies of artificial intelligence and their results.*

***Keywords**: artificial intelligence, object of robotics, subject of crime, electronic person, criminal law measures for electronic persons, crypto currency, Big Data.*

***Аннотация**: В статье рассматриваются вопросы возможности признания искусственного интеллекта (электронного лица) субъектом уголовно-правовых отношений и субъектом преступления, потенциальных информационных и иных угроз со стороны искусственного интеллекта, сохранения контроля над ним, связи информационной безопасности с исследованиями искусственного интеллекта и их результатами.*

***Ключевые слова**: искусственный интеллект, объект робототехники, субъект преступления, электронное лицо, меры уголовно-правового характера по отношению к электронным лицам, криптовалюта, Большие Данные.*

Постановка проблеми. В теорії кримінального права прийнято описувати фізичну особу в якості суб’єкта злочину та її суспільно небезпечну поведінку за допомогою наступних ознак, які одночасно можуть бути пов’язані як з об’єктивною, так і з суб’єктивною стороною злочину: 1) здатність усвідомлювати фактичну сторону; 2) здатність усвідомлювати суспільну небезпечність свого діяння та його наслідків; 3) можливість за конкретних умов здійснення певного вибору між різними варіантами та здатність керувати своєю поведінкою (волимість діяння). М.І. Бажанов визначав волимість як здатність керувати своїми діями [10].

До цього часу всі інші істоти вважалися і вважаються такими, що знаходяться на нижчому по відношенню до людини рівні інтелектуального розвитку, тому питання про визнання їх суб’єктами злочину в площині вітчизняного законодавства не набувало відповідної актуальності. Крім того, триває дискусія щодо можливості визнання суб’єктом злочину юридичної особи, але попри очевидність вирішення цього питання, позитивне його розв’язання вимагатиме внесення системних змін і перегляду окремих усталених положень на рівні теорії кримінального права.

Між тим, можливість створення штучного інтелекту (Artificial Intelligence, скорочено AI), який дорівнює інтелекту людини або перевищує його, є доволі реальною та такою, що може бути досягнута у найближчому майбутньому, у найближчі десятиріччя. Це неминуче викличе необхідність певного переосмислення змісту та ознак поняття суб’єкта злочину.

Результати аналізу наукових публікацій. Дослідженню особливостей феномену суб’єкта злочину було присвячено належну увагу у працях такий вчених, як П.П. Андрушко, Т.М. Арсенюк, М.І. Бажанов, В.М. Бурдін, В.Д. Вознюк, Н.О. Гуторова, В.В. Ємельяненко, О.В. Зайцев, М.Й. Коржанський, М.І. Панов, Є.Л. Стрельцов, В.В. Сташис, В.Я. Тацій, В.І. Тютюгін, В.В. Устименко, М.І. Хавронюк та багатьох інших, питанням інформаційної безпеки в аспекті кримінального права – в роботах Д.С. Азарова, В.І. Борисова, В.М. Брижко, В.К. Грищука, М.В. Карчевського, Є.В. Лащука, С.Я. Лихової, А.А. Музики, В.О. Навроцького, В.Г. Пилипчука, Н.А. Савінової, П.Л. Фріса, В.Б. Харченко та інших, але через свою складність зазначені питання потребують подальшого дослідження.

Метою статті є дослідження ознак штучного інтелекту у співвідношенні до ознак суб’єкта злочину, можливості визнання штучного інтелекту (електронної особи) суб’єктом кримінально-правових відносин та суб’єктом злочину, аналіз окремих потенційних інформаційних та інших загроз з боку штучного інтелекту, можливості та необхідності збереження контролю над останнім, зв’язку інформаційної безпеки з дослідженнями штучного інтелекту та їх результатами.

Виклад основного матеріалу. Здатність фізичної особи як суб’єкта злочину усвідомлювати фактичну сторону означає, що зазначена особа, хоча б у загальних, але достатніх рисах, розуміє хто вона є, де знаходиться, що зараз відбувається і які дії або бездіяльність вона вчинює. Відсутність розуміння зазначених обставин викликають необхідність з’ясувати стан психічного здоров’я цієї особи, чи є вона осудною або ні.

Таке усвідомлення є передумовою можливості здійснити оцінку своєї поведінки з точки зору прийнятої моралі та нормативних приписів: чи є її дії або бездіяльність суспільно корисними, нейтральними, або небезпечними. У останньому випадку здатність до вказаної самооцінки є підставою для кримінально-правового докору згідно до положень ст.ст. 18, 19 КК України.

Можливість за конкретних умов здійснювати вибір між різними варіантами своєї поведінки означає, перш за все, що такий вибір існує (завдати удару або утриматися від нього) на відміну від альтернативного розвитку подій (напр., коли особа, яка випадково втратила рівновагу, позбавлена можливості обрати варіанти поведінки між тим, щоб не піддаватися силі тяжіння та застигнути у повітрі, або тим, щоб надати перевагу падінню). Можливість здійснення вибору та його реалізація утворюють обставину, яку прийнято іменувати волимість діяння. За її відсутності особа не підлягає кримінально-правовому докору (напр., не тягне кримінальної відповідальності спричинення тілесних ушкоджень особою, яка несподівано втратила рівновагу та впала на потерпілого).

Всі інші істоти, з якими сьогодні людина поділяє середовище свого існування, знаходяться поза увагою кримінального права саме в якості суб’єкта злочину, не зважаючи на те, чи здатні вони усвідомлювати фактичну сторону (напр., собака, що надісланий командою свого власника на спричинення ураження іншій особі, напевно розуміє, що відбувається справжня атака на ворога, а не цікава гра), здатні усвідомлювати суспільну небезпечність (або, як найменш, небажаність) свого діяння (напр., собака, який без команди атакує перехожого, пам’ятає через багато чиселенні повторення, що буде підданий покаранню з боку свого володаря за таку небажану для останнього поведінку), чи є у них можливість за конкретних умов здійснення певного

вибору між різними варіантами та чи здатні вони керувати своєю поведінкою. Можливо, що такий традиційний підхід в якості свого підґрунтя, крім іншого, має на рівні підсвідомості та загальних архетипів поведінки визнання людини найвищою істотою серед інших живих істот.

Але так було не завжди і, що найбільш цікаво, є вже не всюди. Щодо давнього та близького минулого достатньо лише пригадати відомі факти, коли раб чи то у Давньому Римі, чи в колоніальній Америці не розглядався в якості рівної людської істоти, а був лише знаряддям (біологічним засобом праці), що не має власних прав та свобод (до речі, останні прояви расової сегрегації ще мали місце у цивілізованих країнах, зокрема – у США, в нещодавні 1950 – 1960 рр.). З іншого боку, не тільки людей визнають вільними істотами, носіями прав і свобод: несподівано для загальної більшості спостерігачів в Індії нещодавно законодавчо визнано дельфінів “особистостями, які не відносяться до людського роду”, у зв’язку з чим вони повинні мати свої власні особливі права, а з їх використанням заборонено заходи у дельфінаріях, акваріумах, океанаріумах тощо [12].

У свою чергу Європейський парламент прийняв на розгляд проект резолюції про правовий статус роботів як “електронної особистості (електронної особи)” [9]. Проект Резолюції передбачає наділення роботів статусом “електронної особистості”, яка має специфічні права та обов’язки. Вказана Резолюція має на меті регулювання правового статусу роботів у суспільстві людей [14]. Актуальність цього питання полягає у тому, що дедалі складніше буде визначати особу (сьогодні це поки що розробник або користувач певного об’єкту робототехніки), яка повинна нести відповідальність за дії з боку штучного інтелекту, наприклад, щодо програмного забезпечення з відкритим початковим кодом (коли його розробниками, або тими, хто його вдосконалює, є невизначена кількість осіб), або відносно штучного інтелекту, який сам себе усвідомлює, наділений здатністю до роздумів про себе та оточуючий світ, самонавчання та самовдосконалення, дбає про власне самозбереження та отримання необхідних ресурсів, має здібності до творчої діяльності, приймає самостійні виважені рішення тощо.

Тому замість того, щоб розташувати штучний інтелект серед вже відомих категорій (фізичні особи, юридичні особи, тварини, речі та інші суб’єкти та об’єкти), пропонується створення нової категорії “електронних осіб” як більш доцільної [18].

Наділення штучного інтелекту статусом “електронної особи”, скоріш за все, не повинне зустріти заперечень та неприйняття у сфері кримінально-правових відносин. Адже не викликає дискусій факт визнання юридичної особи суб’єктом численних правовідносин, в тому числі кримінально-правових. І хоча донедавна вважалося, що юридична особа діє не самостійно, а лише через своїх представників, які врешті-решт і повинні нести кримінальну відповідальність за свої суспільно небезпечні дії або бездіяльність та їх наслідки, але внесенням відповідних змін у КК України було дещо змінено традиційні акценти і нормативно закріплено можливість застосування до юридичної особи заходів кримінального-правового характеру (штраф, загальна конфіскація майна, ліквідація) на підставі положень ст.ст. 96-3, 96-4, 96-6 Розділу XIV-1 “Заходи кримінально-правового характеру щодо юридичних осіб” КК України внаслідок вчинення її уповноваженою особою від імені та в інтересах певної юридичної особи будь-якого із злочинів, передбачених у ст.ст. 209 і 306, ч.ч. 1, 2 ст. 368-3, ч.ч. 1, 2 ст. 368-4, ст.ст. 369, 369-2 КК України, або незабезпечення виконання покладених на її уповноважену особу законом або установчими документами юридичної особи обов’язків щодо вжиття заходів із запобігання корупції, що призвело до вчинення будь-якого із злочинів, передбачених у ст.ст. 209 і 306, ч.ч. 1, 2 ст. 368-3, ч.ч. 1, 2 ст. 368-4, ст.ст. 369, 369-2 КК України, або у випадку вчинення її уповноваженою особою від

імені юридичної особи будь-якого із злочинів, передбачених ст.ст. 258 – 258-5 КК України, або вчинення її уповноваженою особою від імені та в інтересах юридичної особи будь-якого із злочинів, передбачених ст.ст. 109, 110, 113, 146, 147, ч.ч. 2 – 4 ст. 159-1, ст.ст. 160, 260, 262, 436, 437, 438, 442, 444, 447 КК України.

Тому, аби не застосовувати наукове ворожіння [17], вбачається доцільним у кожному випадку зустрічі з чимось новим та(або) несподіваним докладати певних розумових зусиль, покласти край відштовхуванню нових ідей, припинити блокувати свою свідомість від сприйняття фактичних явищ, утриматися від спокуси підміни всього незрозумілого на зручні стереотипи.

Таким чином, доволі прогнозованою вбачається поява в КК України розділу під номером XIV-2 і умовною назвою “Заходи кримінально-правового характеру щодо електронних осіб”, якщо останніх не буде визнано суб’єктом злочину з усіма наступними правовими наслідками такої системної зміни.

Питання щодо можливості визнання суб’єктом злочину вказаної електронної особи або штучного інтелекту виглядає більш провокаційним та революційним. Але у вільній науковій дискусії ніщо не повинно заважати дослідженню будь-якої теоретичної моделі. Отже, відкинемо стереотипи і спробуємо здійснити неупереджений аналіз цього питання.

Спочатку слід звернути увагу на сучасний стан розробок та розвитку штучного інтелекту, а також ті властивості, якими він вже наділений, або буде наділений у найближчому майбутньому.

Сьогодні штучний інтелект використовують в алгоритмах, які фільтрують фоновий шум у слухових апаратах, підказують водіям вірний напрямок руху за навігаційними картами, здійснюють пропозиції споживачам на підставі аналізу їх попередніх замовлень, пропонують новини та аналітичні огляди певної спрямованості на підставі аналізу Великих Даних, підтримують процес прийняття рішень щодо лікування онкологічних захворювань молочної залози, підбирають варіанти лікування та розшифровують електрокардіограми. Крім промислових роботів, існують вже роботи-хірурги, які приймають рішення більш впевнено та ефективно, ніж лікарі – фізичні особи – початківці [4].

Системи розпізнання обличчя людини, мовних, текстових та відеоматеріалів, що побудовані на базі штучного інтелекту, вже є доволі розвинутими і використовуються у багатьох країнах світу. Автоматична ідентифікаційна система вдало працює у Держдепартаменті США, з її допомогою під час видачі віз обробляється більше семідесяти п’яти мільйонів фотографій на рік. Автоматичне доведення математичних теорем та розв’язання рівнянь стали звичайною процедурою для виробників мікропроцесорів під час перевірки поведінки схеми перед її випуском у виробництво. Складні програми календарного планування та тарифікації використовуються у системах бронювання авіаквитків та контролю складських залишків тощо.

Штучний інтелект у перегонах озброєнь досяг таких висот, що відома міжнародна неурядова організація Amnesty International вже почала вимагати від урядів всіх країн заборони розробки роботів-вбивць, які базуються на нових технологіях. За даними Bureau of Investigative Journalism (“Бюро журналістських розслідувань”), в результаті використання безпілотників в період між 2004 та 2013 роками було вбито від 2500 до 3500 осіб, в тому числі мирних жителів і дітей, і більше ніж тисячі завдано поранення [3].

За повідомленням Агенції з перспективних оборонних науково-дослідницьких розробок США (Defense Advanced Research Projects Agency in the United States, DARPA) програма DART у галузі планування та постачання, яка була використана під час

операції “Буря у пустелі”, повністю виправдала тридцятирічне фінансування Міністерством оборони досліджень у галузі штучного інтелекту [6].

Нові потокові котирування цінних паперів, які розробляються агентствами фінансової інформації, спеціально форматуються під інтелектуальні автоматизовані системи. За допомогою алгоритмічного високочастотного трейдінгу, на який припадає значна частка фондового ринку США, існує можливість отримувати прибутки на незначних коливаннях цін у межах декількох мілісекунд (крім того, окремі спостерігачі з Уолл-стріт висловлюють припущення про те, що алгоритми сигналізують один одному та поширюють між собою інформацію за допомогою цих самих мілісекундних угод поза контролем з боку людини [11, с. 46], а відповідальність за так званий миттєвий обвал фондових індексів 6 травня 2010 року покладається саме на алгоритмічну торгівлю [5].

Якщо узагальнити численні різновекторні прогнози, то до 2022 року штучний інтелект буде мислити повністю як людина (а не лише за окремими напрямками) на 10 %, до 2040 року – на 50 %, а до 2075 року його процеси мислення неможливо буде відрізнити від людських так само, як невдовзі складно буде відрізнити між собою штучні та біологічні об’єкти, віртуальні світи стануть більш захоплюючими, ніж реальне оточення [16].

Значно ширший перехід до віртуальних світів невдовзі стане не розвагою, а нагальною потребою і буде виконувати функцію своєрідного соціального клапану. Так, завдяки спрощенню доступу до значного обсягу відомостей та інформаційних потоків неминуче збільшиться обізнаність широких верств населення про нерівність можливостей (неоднаковий доступ до досягнень біології, фармакології, покращення таких когнітивних властивостей, як пам’ять, зір, слух, увага та сила людини, здатність обробляти значні обсяги інформації тощо) та приховані схеми перерозподілу ресурсів з боку вузьких прошарків, що збільшить відкриту відстань між заможними та бідними. Це утворюватиме підґрунтя для невдоволення та можливого соціального вибуху. Зняти соціальну напругу стане можливим якраз через відвернення уваги та переключення її на віртуальні світи. Як це часто буває, оплачувати цей процес випаде на долю тих, кого відволікають. Так само, як сьогодні користувачі добровільно розміщують приватну інформацію про себе в соціальних мережах, оплачують смартфони з розпізнанням відбитків папілярних узорів, використовують пристрої для виміру серцебиття, тиску та інших показників життєдіяльності організму, інформація про що накопичується і стає можливою для узагальненої обробки.

Прогнози щодо появи невдовзі штучного інтелекту, який є рівним інтелекту людині, або навіть перевищує його (суперінтелект – Super Artificial Intelligence, скорочено SAI) виглядають доволі реалістичними також через те, що зазвичай за 5 – 10 років повністю вдосконалюються ті технології, які вже існують на момент прогнозування, а за 15 – 20 років реалізуються ті, що на сьогодні існують лише в якості лабораторних версій та припущень. Слід також пам’ятати про постійне прискорення процесів обміну інформацією, розвитку економічних відносин та революційних технологій, що є найбільш потужними за будь-які інші минулі часи.

Тому людству слід звикнути до того, що неминуче наближається той час, коли людство буде поділяти середовище свого існування з штучним інтелектом.

Не зайвим буде звернути увагу на такі властивості штучного інтелекту, як: 1) здатність до комплексної обробки значних обсягів інформації, здобутої з різних джерел; 2) здатність до самонавчання (в тому числі, накопичування досвіду, узагальнення, відшукування неочевидних зв’язків) та умовиводів; 3) вміння планувати;

4) здатність до роздумів (у відповідь на роздуми розробників про нього, штучний інтелект буде витрачати більш потужні ресурси на роздуми про них [1]) тощо.

Штучний інтелект, так само як і людина, може мати здатність усвідомлювати фактичну сторону того, що відбувається, усвідомлювати суспільну небезпечність свого діяння, яке реалізується в інформаційному просторі або завдяки роботизованим консолям, пристроям або механізмам – в оточуючому матеріальному середовищі (тобто, оцінювати за шкалою “добре – нейтральне – погане”), та, без сумніву, буде мати можливість за конкретних умов здійснювати певний вибір між тими чи іншими варіантами поведінки та здатність керувати своєю поведінкою (сьогодні це є однією з головних умов проведення штучним інтелектом хірургічних операцій, допуску його до керування безпілотними транспортними засобами тощо).

Але, як було зазначено на початку цього дослідження, такі здібності та властивості – це в основному все, що вимагається від людини як суб’єкта злочину в інтелектуальній і вольовій сферах.

Якщо придивитися неупереджено, викладене дає підстави для визнання штучної форми інтелекту та(або) штучної високоорганізованої форми життя (органічної або неорганічної) суб’єктом кримінально-правових відносин та суб’єктом злочину.

Ознаками штучного інтелекту як суб’єкта злочину можуть бути наступні: 1) це є не фізична, а електронна особа (особистість); 2) осудність, що означає у момент вчинення злочину можливість усвідомлювати свої дії (бездіяльність) і керувати ними.

Крім того, у широкому розумінні штучний інтелект може бути наділений такими наступними властивостями (продовження попереднього переліку), які наближають його у межах досліджуваних аспектів до людини, або перевищують здібності останньої: 1) здатність до абстрактного мислення; 2) сприйняття та розпізнання всіх сигналів зовнішнього світу (з свого боку, людина, на відміну від дельфінів та кажанів, не сприймає ультразвук та інфразвук; те, що людина сприймає своїм органом зору, складає лише приблизно 2 % від повного електромагнітного діапазону тощо [13]); 3) потужна теоретична база та самопідготовка (на думку першопрохідника феномену штучного інтелекту А. Тьюрінга концепція повинна полягати у створенні програми, яка отримує більшу частину знань за рахунок навчання, а не завдяки завантаженню первісних даних); 4) стратегічне мислення, здатність заздалегідь прорабляти та прогнозувати різні варіанти; 5) здатність до дедукції та індукції, аналізу та синтезу; 6) здатність моделювати хід думок опонента; 7) здатність ефективно працювати в умовах невизначеності та вірогідності; 8) використання доступної інформації у найбільш доцільний та оптимальний спосіб тощо.

Крім наведеного вище, суперінтелект буде здатний до того, що вже зараз вимагається і від звичайного штучного інтелекту – обізнаність у принципах своєї роботи і завдяки цьому здатність до самовдосконалення (перша версія утворює вдосконалену версію самої себе і так переписує програму до нескінченності), самокопіювання (здатність до поширення і самозбереження), вирішення завдання способом мозкового штурму з залученням багатьох копій самого себе.

У тому випадку, коли чинна версія програми суттєво відрізняється від тієї, яка вийшла свого часу від виробника, складно буде на моральному та правозастосовному рівні виокремити межі відповідальності останнього. У тому випадку, коли штучному інтелекту надається право прийняття остаточного рішення, незважаючи на присутню поруч людину (наведені вище приклади: хірургічна операція, безпека руху транспорту тощо), ще більш складним стає питання визначення суб’єкта відповідальності в звичайних координатах теорії кримінального права.

Крім того, слід врахувати наступне. Якщо штучний інтелект створюється людиною, то його здібності і можливості можуть бути описані у межах світогляду людини, в горизонтах її мозкової діяльності. Якщо суперінтелект буде створений не людиною, а своїм попередником – звичайним штучним інтелектом, то його світогляд та умовиводи можуть бути незрозумілими або незбагненними для людини. На більш простому прикладі це ілюструється наступним: алгоритми, які були розроблені професором Стенфордського університету, піонером у використанні генетичного програмування для оптимізації складних проблем, творцем скретч-карти Джоном Коза (John R. Koza) десятки разів самостійно повторно відтворювали винаходи, які вже були раніше запатентовані людиною-винахідником, а інколи пропонували зайві компоненти, з якими пристрої працювали краще, ніж запропоновані винахідниками-людьми [8].

Але слід підкреслити, що визнання штучного інтелекту суб’єктом злочину буде доцільним та обґрунтованим лише за умови переопрацювання всієї системи кримінального права, в тому числі з питань покарання або інших заходів кримінально-правового характеру. Не слід поспішати за науковою, або політичною модою, бажано уникнути створення так званого законодавчого вірусу [15].

Навряд чи може бути ефективно реалізований щодо штучного інтелекту один з таких важливих різновидів мети покарання, як кара (згідно до положень ч. 2 ст. 50 КК України покарання має на меті не тільки кару, а й виправлення засуджених, а також запобігання вчиненню нових злочинів як засудженими, так і іншими особами). Адже навіть спроба вимкнути електричне живлення може зустріти потужний супротив: як зазначає Джеймс Баррат (James Barrat), автор книги Our Final Invention: Artificial Intelligence and the End of the Human Era (“Наш останній винахід: штучний інтелект і завершення ери людства”), у межах проекту Busy Child людство вперше зіткнулося з розумом, який є більш потужним, ніж розум людини, що усвідомлює себе, переписує власну програму (на її новий варіант витрачається всього декілька хвилин), покращує свій код, знаходить і виправляє помилки, збільшує здатність до засвоєння знань, вирішення завдань і прийняття рішень, вимірює власний коефіцієнт інтелекту IQ за допомогою тестів, готовий до самозбереження (коли розробники комп’ютера відключили його від мережі Інтернет з метою його ізолювання від зовнішнього світу, невдовзі виявилося, що і у цьому стані він продовжував свій розвиток) [11, с. 10].

Так само, по відношенню до штучного інтелекту може виявитися неефективним такий захід як ліквідація, що передбачений стосовно юридичних осіб відповідно до положень ст.ст. 96-3, 96-4, 96-6 Розділу XIV-1 “Заходи кримінально-правового характеру щодо юридичних осіб” КК України. Якщо штучний інтелект буде розосереджений у просторі за технологією blockchain (блочні ланцюжки) [7], яка є відомою вже багато років, а сьогодні створює можливість для існування, використання та розповсюдження криптовалют (таких як Bitcoin, Ethereum, Litecoin, Namecoin, Ripple, Dash, NEM, Monero та інші [2]), здатність людини до знищення штучного інтелекту буде прямувати до нуля.

Тому, швидше за все, більш ефективним стане вектор розвитку системи покарань або інших заходів кримінально-правового впливу у напрямку компенсаторних економічних важелів за рахунок активів та можливостей самого штучного інтелекту (напр., стягнення на користь держави, компенсація потерпілому) – сплата певної грошової суми у звичайній валюті, транзакція криптовалютою, виконання робіт, надання послуг тощо.

Не менш важливим є питання про те, що у випадку збереження контролю над штучним інтелектом (відносно чого є бажання все ж таки сподіватися на позитивний розвиток подій), чи буде людина сама реалізовувати відповідні заходи відповідальності та(або) впливу, або доручить їх застосування іншим різновидам штучного інтелекту.

Насправді, під час проектування штучного інтелекту ніщо не заважає закласти в нього таке ядро, завдяки якому за будь-яких умов були б захищені всі або основні загальнолюдські цінності. Але тоді зникає сенс розробки певних видів озброєнь та систем отримання переваг в економічній конкуренції. Тому навряд чи розробники, серед яких багато державних та недержавних потужних корпорацій, погодяться на такий крок. Навіть в більш простій ситуації дорожньо-транспортної події ми не можемо дати раду тому, як повинен повести себе штучний інтелект, що керує транспортним засобом: за будь яких умов рятувати пасажирів, незважаючи на втрати пішоходів та інших учасників дорожнього руху, або діяти навпаки, зважуючи розмір шкоди спричиненої та відвернутої в умовах крайньої необхідності на підставі положень ст. 39 КК України (в останньому випадку пасажири можливо не будуть згодні довіряти своє життя та здоров’я такому безпілотному транспортному засобу, для якого загибель пасажира буде розглядатися меншою шкодою, ніж відвернення смерті двох пішоходів).

Якщо утопічно припустити, що всі розробники між собою домовилися про розробку вказаного ядра, то все одно виникає питання, узгодити яке буде вкрай важко: яким чином в конкретній ситуації визначити, що один з опонентів діє врозріз з загальнолюдськими цінностями (адже навіть під час замаху на позбавлення життя вчинене може вважатися цілком правомірною поведінкою у межах необхідної оборони відповідно до положень ст. 36 КК України)?

Під час розробки зазначеного ядра, велика моральна відповідальність відносно якого перед усім людством покладається не тільки і не стільки на фахівців в сфері робототехніки та програмування штучного інтелекту, але й на представників інших галузей та дисциплін – філософів, соціологів, правників тощо, слід звернути увагу також на наступне: 1) декілька звичайних гарно прописаних та обґрунтованих алгоритмів у своїй сукупності можуть привести до непередбачуваного результату (перехід кількості в якість, але з негативним відтінком); 2) припущення та приписи, які виглядають цілком розумними та логічними, і, як наслідок, є планом до вчинення певних дій, у непередбачуваній ситуації можуть виявитися невдалими, але програма буде продовжувати їх виконувати будь за всяку ціну; 3) у занадто короткий проміжок часу людина може не встигнути відреагувати на певну ситуацію (як під час згадуваної кризи миттєвого обвалу фондових індексів 6 травня 2010 року), тож треба передбачити відповідні алгоритми блокування та можливості виправлення (повернення до попереднього стану).

Висновки та пропозиції.

Враховуючи вищевикладене, вбачаються підстави до наступних висновків та пропозицій: 1) перенесення значного сектору життєдіяльності людини до віртуальних світів є неминучою подією, в тому числі передбачуваною в якості певного соціального клапану; 2) віртуальним світом та повсякденним життям (роботою програм, механізмів, приладів, обладнання) у найближчому майбутньому може повністю опікуватися штучний інтелект (Artificial Intelligence, скорочено AI) або суперінтелект (Super Artificial Intelligence, скорочено SAI), який стане більш розумним, досконалим та усвідомленим за людину; 3) штучний інтелект (електронна особа, особистість) може бути наділений здатністю усвідомлювати фактичну сторону, усвідомлювати суспільну небезпечність своєї дії або бездіяльності та їх наслідків, керувати своєю поведінкою за

можливість вибору (наявність декількох варіантів поведінки); 4) штучний інтелект (електронна особа, особистість) може бути визнаний суб’єктом злочину; 5) визнання штучного інтелекту (електронної особи, особистості) суб’єктом злочину буде доцільним та обґрунтованим лише за умови переопрацювання всієї системи кримінального права поза спокусливого наслідування науковій або політичній моді.

Перспективи подальших досліджень. Розглянуті питання та надана їм авторська оцінка є дискусійними та відкритими для широкого обговорення з огляду на їх актуальність та важливість для забезпечення сталого розвитку суспільства і збереження людства.

Використана література

1. Barrat James. Our Final Invention: Artificial Intelligence and the End of Human Era. – Mode of access : http://www.tor.com/2013/09/20/our-final-invention-excerpt. – Title from the screen.
2. CryptoCurrency Market Capitalizations. – Mode of access : https://coinmarketcap.com. – Title from the screen.
3. Drone War – The bureau of investigative journalism. – Mode of access : https://www.thebureauinvestigates.com/projects/drone-war. – Title from the screen.
4. Executive Summary of World Robotics 2011 Industrial Robots & World Robotics 2011 Service Robots. – Mode of access : http://www.diag.uniroma1.it/~deluca/rob1_en/2011_WorldRobotics_ExecSummary.pdf. – Title from the screen.
5. Findings Regarding the Market Events of May 6, 2010 – Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues. – Mode of access : https://www.sec.gov/news/studies/2010/marketevents-report.pdf. – Title from the screen.
6. Hedberg Sara Reese. Dart: Revolutionizing Logistics Planning // IEEE Intelligent Systems, 2002, 17 (3). P. 81-83. – Mode of access : http://ieeexplore.ieee.org/document/1005635. – Title from the screen.
7. Hodson H. Bitcoin moves beyond mere money / New Scientist. 20 November 2013. – Mode of access: https://www.newscientist.com/article/dn24620-bitcoin-moves-beyond-mere-money. – Title from the screen.
8. Koza, J.R.; Keane, M.A.; Streeter, M.J.; Mydlowec, W.; Yu, J.; & Lanza, G. Genetic Programming IV: Routine Human-Competitive Machine Intelligence. Springer, 2003. – Mode of access : http://www.springer.com/la/book/9780387250670. – Title from the screen.
9. Wakefield J. MEPs vote on robots' legal status - and if a kill switch is required. – Mode of access : http://www.bbc.com/news/technology-38583360. – Title from the screen.
10. Бажанов М.І. Кримінальне право України : підручник / М.І. Бажанов. – К. : Юрінком Інтер, 2005. – Режим доступу : http://www.ebk.net.ua/Book/KPravo/10-15/10145.htm. – Заголовок з екрану.
11. Баррат Дж. Последнее изобретение человечества : искусственный интеллект и конец эры Homo sapiens. – М. : Альпина Нон-фикшн, 2015. – 304 с.
12. Индия признала дельфинов личностями и запретила дельфинарии. – Режим доступу : http://econet.ru/articles/78180-indiya-priznala-delfinov-lichnostyami-i-zapretila-delfinarii. – Заголовок з екрану.
13. Иллюзия восприятия: ограниченность зрения, слуха и других органов чувств человека. – Режим доступу : http://bp21.livejournal.com/103392.html. – Заголовок з екрану.
14. Коваль М. Электронная личность : зачем ЕС обсуждает права роботов. – Режим доступу : http://www.eurointegration.com.ua/rus/experts/2017/01/24/7060539. – Заголовок з екрану.
15. Киричко В.М. Законодавчий вірус у системі КК України : визначення і актуалізація проблеми на прикладі ст.368-2 КК “Незаконне збагачення” // Проблеми законності : зб. наук. праць ; відп. ред. В.Я. Тацій. – Харків : Нац. юрид. ун-т імені Ярослава Мудрого, 2016. – Вип. 133. – 282 с.

16. Радутний О.Е. Кримінальна відповідальність юридичної особи стане кроком до закріплення віртуальності життєвого простору // Електронне наукове фахове видання Національного університету “Юридична Академія України ім. Ярослава Мудрого”. – № 1/2011. – Режим доступу : http://nauka.jur-academy.kharkov.ua. – Заголовок з екрану.

17. Радутний О.Е. Стан інформаційно-законодавчої діяльності на прикладі Кримінального кодексу України // Інформація і право. – № 3(18)/2016. – С. 58-67.

18. Хель И. Права роботов : когда разумную машину можно считать “личностью”. – Режим доступу : https://hi-news.ru/robots/prava-robotov-kogda-razumnuyu-mashinu-mozhno-schitat-lichnostyu.html. – Заголовок з екрану.

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

УДК 347.132

ЄВТУШЕНКО Є.В., провідний науковий співробітник Центру судових і спеціальних експертиз Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України

ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України.

НЕДІЙСНІСТЬ ПРАВОЧИНУ У ЦИВІЛЬНОМУ СУДОЧИНСТВІ

Анотація. *У статті досліджуються актуальні питання, що пов’язані з визнанням правочину недійсним. Аналізується законодавство про недійсний та оспорюваний правочин. На базі аналізу узагальнення судової практики пропонуються зміни до порядку визнання недійсності правочину.*

Ключові слова: *правочин, недійсний правочин, оспорюваний правочин, нікчемний правочин.*

Summary*. The article deals with topical issues related to the recognition of a transaction as invalid. The law on controversial and insignificant transactions is analyzed. On the basis of an analysis of the generalization of judicial practice, changes are proposed to the recognition of the fact of invalidity of the transaction.*

Keywords: *transaction, invalid transaction, contested transaction, insignificant transaction.*

Аннотация. *В статье исследуются актуальные вопросы, связанные с признанием сделки недействительной. Анализируется законодательство об оспариваемых и ничтожных сделках. На основании анализа обобщения судебной практики предлагаются изменения порядка признания факта ничтожности сделки.*

Ключевые слова: *сделка, недействительная сделка, оспариваемая сделка, ничтожная сделка.*

Постановка проблеми. Згідно зі ст. 1 Цивільного процесуального кодексу України 2004 р. (далі – ЦПК України) одним із основних завдань цивільного судочинства є охорона порушених, невизнаних або оспорюваних прав фізичних, юридичних осіб, держави шляхом всебічного розгляду та вирішення цивільних справ. Відповідно, важливого значення набуває правильне тлумачення судом деяких елементів предмета спору, від чого, зрозуміло, залежить кінцевий результат – рішення по справі.

Інститут правочину (правочин – дія особи, спрямована на набуття, зміну або припинення цивільних прав і обов’язків) став новелою для Цивільного кодексу України 2003 р. (далі – ЦК України), зайнявши центральне місце в системі цивільного права, у зв’язку з чим значної актуальності сьогодні набуває поняття “недійсності” правочину, про що свідчать статистичні дані, наведені в узагальненій судовій практиці Верховного Суду України “Практика розгляду судами цивільних справ про визнання правочинів недійсними” від 24 листопада 2008 року, де вказується, що в 2007 р. у провадженні судів перебувало 19,7 тис. справ цієї категорії, або 1,5 % – від загальної кількості цивільних справ позовного провадження. Надходження до судових інстанцій позовів такого характеру невпинно зростає, оскільки за даними Єдиного державного реєстру судових рішень за 2010 – 2016 рр. було ухвалено 25,18 тис. рішень щодо справ про визнання правочинів (в т. ч. договорів) недійсними.

З огляду на це, залишається питання, щодо яких саме правочинів судами застосовується поняття “недійсний”, зокрема, в яких випадках суди звертаються до їх поділу на види – нікчемний та оскаржений.

Результати аналізу наукових публікацій. Питаннями щодо визначення поняття “недійсності” правочину в матеріальному праві займалися такі вчені та практики юриспруденції, як Давидова І.В., Перова О.В., Гусак М.В., Хатнюк Н.С., Петровський А.В., Саніахметова Н.О. та інші.

Водночас, основна увага науковців була спрямована на матеріальний аспект недійсності правочинів [1, с. 84]. Очевидним залишається те, що наукові розробки щодо процесуального аспекту визнання правочинів недійсними за українським законодавством фактично відсутні. Таким чином, вивчення проблеми застосування поняття недійсності правочину в цивільному судочинстві є актуальним та потребує наукового дослідження.

Метою статті є удосконалення на базі аналізу цивільного законодавства та узагальнення судової практики порядку визнання недійсності правочину.

Виклад основного матеріалу. Загальновідомо, що основною метою визнання правочину недійсним є анулювання майнових наслідків його вчинення та встановлення наслідків, передбачених законом. Крім того, інститут визнання правочину недійсним стимулює осіб дотримуватись положень, вже закріплених законодавством; запобігає зловживанню правами; є орієнтиром для вчинення правочинів згідно з вимогами права та чинного законодавства; охороняє права та законні інтереси учасників цивільних правовідносин. Враховуючи основні принципи цивільного права, з урахуванням ст.ст. 203, 204 ЦК України, недійсність правочину може бути передбачена виключно законами України, що прийняті відповідно до Конституції України, актами Президента України, постановами Кабінету Міністрів України, актами органів державної влади України, органів АР Крим, що видаються у випадках та в межах, встановлених Конституцією та законами України. Отже, будь-який правочин, що не відповідає вимогам законодавства, повинен визнаватись судами як недійсний.

В українській мові термін “недійсний” має таке значення: який не має законної сили; який не існує; не реальний. Недійсним є правочин, який хоч і спрямований на набуття, зміну або припинення цивільних прав та обов’язків, але не створює таких наслідків у зв’язку із невідповідністю цих дій вимогам актів цивільного законодавства. Недійсність правочину зумовлюється наявністю дефектів його елементів:

1) дефекти (незаконність) суб’єктного змісту правочину;

2) дефекти недотримання форми;

3) дефекти суб’єктного складу;

4) дефекти волі – невідповідність волі та волевиявлення.

Постановою Пленуму Верховного Суду України “Про судову практику розгляду цивільних справ про визнання правочинів недійсними” від 6 листопада 2009 року № 9 визначено, що судам, відповідно до ст. 215 ЦК України, необхідно розмежовувати види недійсності правочинів: нікчемні правочини – якщо їх недійсність встановлена законом (ч. 1 ст. 219, ч. 1 ст. 220, ч. 1 ст. 224 тощо), та можливість оскаржувати їх недійсність прямо не встановлена законом, але одна із сторін або інша заінтересована особа заперечує їх дійсність на підставах, встановлених законом (ч. 2 ст. 222, ч. 2 ст. 223, ч. 1 ст. 225 ЦК України тощо).

Нікчемний правочин в науці цивільного права іноді називають “мертвонародженим” [3, с. 62], оскільки він із самого початку не породжує передбачених законом правових наслідків незалежно від пред’явлення позову про визнання його недійсним. За нормами ЦК України нікчемними правочинами є:

1) укладені з недодержанням обов’язкової письмової форми, якщо недійсність прямо передбачена законом, а саме: ст.ст. 547, 719, 981, 1055, 1059, 1107, 1118 ЦК України тощо;

2) укладені з недодержанням обов’язкової нотаріальної форми та/або які підлягають обов’язковій державній реєстрації – ст.ст. 210, 219, 640, 1257 ЦК України, але у виняткових випадках, встановлених ст.ст. 218 та 220 ЦК України такі правочини, окрім визнання дійсним заповіту, який є нікчемним у зв’язку із порушенням вимог щодо форми його недійсності, можуть бути визнані дійсними в судовому порядку;

3) укладені із малолітньою особою, за межами її цивільної дієздатності без належного схвалення – ст. 221 ЦК України; правочин, вчинений без дозволу органу опіки та піклування – ст. 224 ЦК України;

4) укладені недієздатною фізичною особою – ст. 226 ЦК України;

5) правочини, які порушують публічний порядок, тобто які посягають на суспільні, економічні та соціальні основи держави, спрямовані на порушення конституційних прав і свобод людини і громадянина та на знищення, пошкодження майна фізичної, юридичної особи, держави, Автономної Республіки Крим, територіальної громади – ст. 228 ЦК України.

Наведений перелік нікчемних правочинів не є повним, адже ЦК України та іншими законодавчими актами встановлено також інші підстави нікчемності правочинів. Деякі фахівці цивільного права вважають, що для визнання нікчемного правочину “недійсним” немає необхідності в рішенні суду [4, с. 34], крім того, існує безліч судових рішень про залишення позовних заяв без руху на тій підставі, що нікчемний правочин є недійсним через невідповідність його вимогам закону та не потребує визнання його судом. Звісно, існування такої законодавчо закріпленої норми суттєво розвантажує діяльність судів, проте на практиці застосування ч. 2 ст. 215 ЦК України має свої недоліки. Погоджуючись з цією думкою, необхідно зазначити, що “автоматична” *(ipso facto)* нікчемність правочину не витримує жодної критики з точки зору гарантій стабільності та передбачуваності цивільних правовідносин [4, с. 34].

Висновок щодо відповідності того чи іншого правочину вимогам закону дуже часто потребує ґрунтовного юридичного аналізу, а отже, це є справою суду. Чинна редакція ч. 2 ст. 215 ЦК України дає можливість посадовим особам державних органів на власний розсуд оголошувати будь-який із вищенаведених правочинів недійсним без звернення до суду та ігнорувати його. Становище ускладнюється й тим, що законодавцем у цій статті не наведено конкретного переліку нормативних актів, якими повинна визначатися недійсність, тому систематично вносяться зміни до них та з’являються нові закони. Необхідність у визнанні правочину нікчемним у судовому порядку виникає і тоді, коли відповідний правочин має ознаки діючого, проте містить невидимі недоліки та відповідно здійснюються інші юридичні дії. Відповідно, задля усунення зовнішніх ознак дійсності правочину та недопущення в майбутньому фактичних змін у праві (набуття/володіння/інше) виникає необхідність у судовому підтвердженні недійсності. Постанова Пленуму Верховного Суду України від 6 листопада 2009 року № 9 та постанова Пленуму Верховного Суду України “Про судову практику у справах про спадкування” від 30 травня 2008 року № 7 визначають таке: вимога про встановлення нікчемності правочину підлягає розгляду в разі наявності відповідного спору. Позов про це може пред’являтися окремо, без застосування наслідків недійсності нікчемного правочину, в цьому разі суд у резолютивній частині рішення вказує про нікчемність правочину або відмову в цьому. Також потреба у визнанні правочину нікчемним може виникнути у разі, коли: сторони виконали певні умови нікчемного правочину, який нотаріально засвідчений; порушує права третіх осіб; зареєстрований у державних органах тощо. У таких випадках рішенням суду можуть бути визначені відповідні правові наслідки недійсності правочину. Варто зауважити, що норми ст. 215 ЦК України

щодо підстав нікчемності правочинів є імперативними, тобто такими, що містять підставу для відмови у визнанні мирової угоди. Згідно зі ст. 215 ЦК України іншим видом недійсності правочинів є оспорюваний правочин. Такий правочин може бути визнаний недійсним лише судом, якщо недійсність правочину прямо не встановлена законом, але одна із сторін або інша заінтересована особа заперечує його дійсність на підставах, встановлених законом, такий правочин може бути визнаний судом недійсним (оспорюваний правочин). На відміну від нікчемного, оспорюваний правочин на момент створення породжує для його сторін цивільні права та обов’язки, а тому вважається дійсним, хоча за своєю суттю він також є протизаконним. Водночас порушення умов дійсності правочинів на момент набуття дає можливість одній зі сторін або заінтересованій особі звернутися до суду із позовом про визнання такого правочину. На думку Хатнюк Н.С., оспорювані правочини – це правочини з вадами волі [5]. Так, правочини визнаються недійсними внаслідок того, що волевиявлення не відображає волю учасника правочину, а волю будь-якої іншої особи, яка впливає на учасника правочину. Тому законодавство передбачає підстави, для їх оспорювання з причини або неповноцінності самої волі особи, яка здійснила (уклала) правочин, або, зважаючи на вплив різних тяжких обставин, що склалися у волевиявленні [6, с. 776]. Зокрема, до оспорюваних ЦК України відносить правочини:

1) вчинені неповнолітньою особою за межами її цивільної дієздатності – ст. 222 ЦК України;

2) вчинені фізичною особою, цивільна дієздатність якої обмежена – ст. 223 ЦК України;

3) вчинені дієздатною фізичною особою, яка у момент його вчинення не усвідомлювала значення своїх дій та/або не могла керувати ними – ст. 225 ЦК України;

4) вчинені юридичною особою, без відповідного дозволу/ліцензії – ст. 227 ЦК України;

5) вчинені під впливом помилки – ст. 229 ЦК України;

6) вчинені під впливом обману – ст. 230 ЦК України;

7) вчинені під впливом насильства – ст. 231 ЦК України;

8) вчинені в результаті зловмисної домовленості представника однієї сторони з іншою стороною – ст. 232 ЦК України;

9) вчинені під впливом важких обставин – ст. 233 ЦК України;

10) фіктивний – ст. 234 ЦК України;

11) удаваний – ст. 245 ЦК України.

Процес оспорювання зазначених правочинів передбачає доказування певного факту, що має значення для дійсності правочину. Наприклад, при задоволенні позову про визнання недійсним правочину, вчиненого юридичною особою без необхідного на те дозволу, доцільним є витребування у позивача доказів, які підтверджують, що відповідач знав чи зобов’язаний був знати про невідповідність правочину вимогам законодавства, що правочин укладений без ліцензії на заняття певними видами діяльності. Обов’язковому доказуванню підлягають питання, пов’язані з наявністю чи відсутністю волі та правильним її відображенням у волевиявленні. Так, передбачені ст.ст. 229 – 233 ЦК України заявлені вимоги можуть бути задоволені за умови доведення факту обману, насильства, погрози, зловмисної домовленості представника однієї сторони з іншою, збігу важких обставин і наявністю їх зв’язку із волевиявленнями сторони вчинити правочин на вкрай невигідних для неї умовах. Відповідно, якщо при визнанні в судовому порядку правочину фіктивним будуть наявні докази щодо передачі майна за договором, який не може бути кваліфікований як

фіктивний, а відповідно, і як недійсний. На відміну від нікчемних правочинів, при визнанні правочинів недійсними та застосуванні наслідків їх недійсності мирові угоди визнаються судами з урахуванням вимог ст. 175 ЦПК України.

Враховуючи вищевикладене, необхідно звернути увагу на те, що недійсний правочин — це акт, який все ж таки звершився, але в силу визначених у ньому законодавством недоліків та/чи рішення суду, він не має правової сили. Тож при розгляді спорів про недійсність правочинів судами, необхідно розмежовувати недійсні правочини та неукладені, оскільки неукладені правочини за своєю суттю існувати не можуть, а тому правової сили не мають. Так, не є укладеними правочини, у яких відсутні встановлені законодавством вимоги, потрібні для їх укладення: відсутня згода за всіма істотними умовами договору; не отримано акцепт стороною, що отримала оферту; не передано майно, якщо відповідно до законодавства необхідна його передача; не затверджено правочин вищим органом господарського товариства, якщо це передбачено в статуті тощо.

Проаналізувавши норми ЦК України, постанову Пленуму Верховного Суду України “Про судову практику розгляду цивільних справ про визнання правочинів недійсними” від 6 листопада 2009 року № 9, узагальнення Верховного Суду України “Практика розгляду судами цивільних справ про визнання правочинів недійсними” від 24 листопада 2008 року, вважаємо, що на даний час поняття “недійсності” правочинів є детально визначеним, у тому числі шляхом розмежування понять “нікчемний правочин” та “оспорюваний правочин”, бо кожен з видів недійсності правочинів передбачає різні юридичні наслідки. Незважаючи на те, що порядок визнання недійсності правочину в цивільному судочинстві є дещо ускладненим, що зумовлює його неоднакове застосування судами різних інстанцій при винесенні рішень, сподіваємося, що за умови внесення законодавцем відповідних змін до ЦК України, Вищим спеціалізованим судом України надалі буде постійно оновлюватися узагальнення судової практики цієї категорії справ. Положення ст. 4 ЦПК України встановлюють єдиний та основний обов’язок цивільного судочинства – захист прав, свобод та інтересів фізичних, юридичних осіб тощо, які знаходять своє продовження у ст. 16 ЦК України, де закріплено один із способів захисту цивільних прав та інтересів – визнання правочину недійсним, що передбачає винесення рішення судом при задоволенні відповідного позову. Натомість ст. 215 ЦК України припускає можливість не визнавати недійсним нікчемний правочин. Таким чином, виникають суперечності між положеннями ЦПК України, які встановлюють можливість і способи захисту цивільних прав та інтересів осіб, і положеннями ст. 215 ЦК України .

З огляду на наведене, вважаємо, що вирішуючи питання про визнання недійсним правочину, суди повинні звертати увагу на п. 5 постанови Пленуму Верховного Суду України “Про судову практику розгляду цивільних справ про визнання правочинів недійсними” від 06 листопада 2009 року № 9 та чітко розмежовувати, до якого виду належить правочин, визнання недійсним якого вимагає позивач, і залежно від встановлення вказаних обставин ухвалювати рішення про задоволення позову чи відмову у його задоволенні.

Висновки.

З метою удосконалення цивільного законодавства пропонуємо внести зміни до ст. 215 ЦК України шляхом вилучення другого речення частини 2 цієї статті, а саме: “У цьому разі визнання такого правочину недійсним судом не вимагається”.

Зазначене усуне наявні суперечності у цивільному законодавстві та сприятиме ухваленню судами рішень, які підтверджуватимуть нікчемність правочину.

Використана література

1. Петровський А.В. Еволюція наукових думок щодо матеріального та процесуального аспекту визнання правочинів недійсними // Юридична наука. – 2011. – № 3. – С. 79-86.

2. Аналіз окремих питань судової практики, що виникають при застосуванні судами рекомендаційних роз’яснень, викладених у постанові Пленуму Верховного Суду України від 06 листопада 2009 року № 9 “Про судову практику розгляду цивільних справ про визнання правочинів недійсними”. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cg

3. Перова О.В. Недійсність правочину, який порушує публічний порядок : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.03 / О.В.Перова/ – Х., 2010. – 15 с.

4. Федорчук Д. Новели законодавства щодо підстав визнання правочинів недійсними // Юридичний радник. – № 3(11). – 2006. – С. 97-103.

5. Хатнюк Н.С. Юридична природа нікчемних правочинів. – Режим доступу : http://www.nbuv.gov.ua/portal/soc_gum/pre/2008/Hatnyuk.pdf

6. Харитонов Є.О. Цивільне право України : підруч. / Є.О. Харитонов, Н.О. Саніахметова. – К. : Істина, 2003. – 776 с.

7. Гусак М., Данішевська В., Попов Ю. Нікчемні та оспорювані правочини : регулювання за Цивільним кодексом України // Право України. – 2009. – № 6. – С.37

8. Давидова І.В. Види недійсних правочинів. – Режим доступу : http://vuzlib.com/content/view/1438/126

9. Про судову практику у справах про спадкування : Постанова Пленуму Верховного Суду України від 30.05.08 р. № 7. – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi

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

УДК 343.2/.7(477)(045)

ОВЧІННІКОВ Р.М., студент Навчально-наукового Юридичного інституту
Національного авіаційного університету

ВІЙСЬКОВІ ЗЛОЧИНИ: ПРАВОВЕ РЕГУЛЮВАННЯ ТА ШЛЯХИ УДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ

Анотація. *У статті тлумачиться поняття військового злочину, види цих злочинів та відповідальності за їх вчинення. Проаналізовано погляди різних науковців стосовно правового регулювання кримінального законодавства з даної теми та розглянуто шляхи вдосконалення. Особлива увага зосереджена на проблемах застосування кримінально-правових норм стосовно військових злочинів.*

Ключові слова: *військові злочини, види військових злочинів, система військових злочинів, реформування.*

Summary. *The article will interpret the concept of a war crime, the types of these crimes and the responsibility for their commission. The views of different scholars on the legal regulation of criminal legislation on this topic are analyzed and ways of improvement are considered. The attention is also concentrated on the problems of the application of criminal law in relation to war crimes.*

Keywords: *war crimes, types of war crimes, system of war crimes, reformation.*

Аннотация. *В статье объясняется понятие военного преступления, виды этих преступлений и ответственности за их совершение. Проанализированы взгляды разных ученых относительно правового регулирования уголовного законодательства по данной теме и рассмотрены пути усовершенствования. Также особое внимание сосредоточено на проблемах применения уголовно-правовых норм в отношении военных преступлений.*

Ключевые слова: *военные преступления, виды военных преступлений, система военных преступлений, реформирование.*

Постановка проблеми. Заходи щодо захисту та реалізації інтересів національної безпеки, забезпечення стабільного функціонування політичних та економічних систем держави потребують високого рівня ефективності боротьби зі злочинною діяльністю у військовій сфері та сприянню закріплення правового режиму в ній. Внесення відповідних змін до Кримінального кодексу України (далі – КК України) пов’язане зі своєчасною та ефективною реакцією законодавства на загрозу інтересам держави та безпеці її громадян.

Реалізація військово-правової реформи в Україні ставить перед законотворцями та перед вітчизняною юридичною наукою багато питань. Більшість із них потребують широкого теоретичного дослідження. При виконанні завдань, що покладаються на Збройні Сили України, важливу роль відіграють службові особи, які формують військово-адміністративний апарат і наділені певними повноваженнями в частині командно-організаційної та адміністративної діяльності. Надаючи військовим особам певні службові та владні повноваження, закон вимагає, щоб вони використовувались виключно на благо військової служби. Тому при здійсненні злочину під час несення військової служби ці особи грубо порушують ст. 17 Конституції України [1], закони України та Військову присягу, яка вимагає сумлінного та чесного виконання свого військового обов’язку.

Результати аналізу наукових публікацій. Вирішенню проблем військово-кримінального законодавства України та відповідальності за вчинення військових злочинів приділяли увагу наступні науковці: Г.М. Анісімов, Ю.П. Дзюба, В.І. Касинюк,

М.І. Панов, М.Г. Колодяжний, В.І. Баулін, В.І. Борисов, В.І. Тютюгін, Н.О. Гуторова, О.М. Сарнавський, О.В. Черниш та інші. Проте, в умовах глобалізації злочинності кримінальне право України потребує подальшого його удосконалення.

Метою статті є дослідження змісту військового злочину в кримінальному праві України, його ознак, передбачених КК України, оцінка здобутків вчених та визначення шляхів законодавчого удосконалення.

Виклад основного матеріалу. Профілактика та протидія злочинності у військовій сфері є частиною кримінально-правової політики України. КК України містить сукупність норм, якими здійснюється кримінально-правове регулювання суспільних відносин, що стосуються військовослужбовців, як носіїв, визначених військовим законодавством, конкретних прав та обов’язків. Цей комплекс включає норми Загальної та Особливої частини КК України. Ефективність зазначеного кримінально-правового регулювання залежить від їх узгодженості між собою, а також від узгодженості з іншими нормами в частинах КК України, як підсистеми кримінального права. Впровадженню законодавчих змін або доповнень до цих норм повинні передувати наукові дослідження та всебічний аналіз статистики військових злочинів, скоєних військовослужбовцями.

У загальній частині КК України специфіка кримінально-правової регламентації суспільних відносин, що стосується військовослужбовців, була втілена в нормах інститутів покарання і судимості. Об’єктом згаданих відносин є поведінка їх учасників (дії або утримання від дій). У переліку видів покарань, як визначено в ст. 51 КК України, передбачено покарання у виді службового обмеження для військовослужбовців (п. 6) та тримання в дисциплінарному батальйоні військовослужбовців (п.10).

Перше із них може бути застосовано до всіх категорій військовослужбовців, крім осіб, які проходять строкову військову службу. В свою чергу, друге – застосовується лише для військовослужбовців строкової служби. Арешт – вид покарання, який застосовується щодо військовослужбовців, визначається законодавцем як гауптвахта у ч. 2 ст. 60 КК України. Виконання кримінального покарання для військовослужбовців у формі арешту, а також у формі затримання їх в дисциплінарному батальйоні, є функцією Військової служби правопорядку у Збройних Силах України.

Також варто відзначити застосування покарання до військовослужбовців у вигляді позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу (ст. 54 КК України), яке застосовується як додаткова форма покарання. Військовослужбовець може бути позбавлений військового звання за вироком суду, якщо він був притягнутий до відповідальності за вчинення тяжкого чи особливо тяжкого злочину. Норми інституту покарання також передбачають певні застереження стосовно військовослужбовців. Такі види покарань, як громадські роботи та обмеження свободи, не можуть застосовуватися до осіб, які проходять строкову військову службу (ч. 3 ст. 56 та ч. 3 ст. 61 КК України). Усі, без винятку, категорії військовослужбовців не підлягають застосуванню покарання у вигляді виправних робіт (ч. 2 ст. 57 КК України).

У питаннях звільнення від покарання придатність до військової служби за станом здоров’я має значення для військовослужбовців, засуджених до службового обмеження, арешту та тримання в дисциплінарному батальйоні (ч. 3 ст. 84 КК України).

Окремого врегулювання набули й питання погашення судимості військовослужбовців. Згідно з ч. 4 ст. 89 (Строки погашення судимості) КК України такими, що не мають судимості, визнаються особи, які відбули покарання у виді службового обмеження для військовослужбовців або тримання в дисциплінарному

батальйоні військовослужбовців чи достроково звільнені від цих покарань, а також військовослужбовці, які відбули покарання на гауптвахті замість арешту.

Конструюючи вищезазначені норми та розміщуючи їх в Загальній частині КК України у розділах “Покарання та його види” (X), “Звільнення від покарання та його відбування” (XII) та “Судимість” (XIII), законодавець мав спрямувати свої зусилля на досягнення не тільки досконалості їх конструкцій, а й узгодженості між собою та з іншими нормами в межах вказаних інститутів Загальної частини КК України.

На нашу думку, окреслена мета в цілому законодавцем досягнута. Разом із тим, слід констатувати, що окремі положення цього комплексу норм все ж заслуговують на критику, зокрема, положення ч. 4 ст. 89 КК України.

По-перше, законодавець у цьому пункті передбачає погашення судимості військовослужбовцям з моменту їх дострокового звільнення від відбування покарання у виді тримання в дисциплінарному батальйоні військовослужбовців, яке є більш суворим, ніж арешт, а також передбачає таке погашення і військовослужбовцям, які достроково звільнені від відбування покарання у виді службового обмеження для військовослужбовців, яке є менш суворим, ніж арешт. Водночас для військовослужбовців, які достроково звільнені від відбування покарання, проміжного за критерієм ступеня суворості, тобто від арешту, законодавець погашення судимості не передбачає. Така позиція законодавця виглядає нелогічною.

По-друге, має місце термінологічна неузгодженість у межах пункту. Терміни, які застосовуються у ньому стосовно суб’єктів відбування покарань, потребують уніфікації. Законодавець називає суб’єктів, які відбули покарання у виді службового обмеження для військовослужбовців та у виді тримання в дисциплінарному батальйоні військовослужбовців, особами, а суб’єктів, які відбули покарання у виді арешту – військовослужбовцями.

По-третє, у пункті зазначено, що такими, що не мають судимості, визнаються військовослужбовці, які відбули покарання на гауптвахті замість арешту. Вказане формулювання суперечить положенням п. 8 ст. 51 та ч. 2 ст. 60 КК України, адже гауптвахта є місцем відбування арешту, а не заміною йому [1, с. 309-310]. Перераховані недоліки, на нашу думку, мають бути взяті до уваги законодавцем та усунуті в ході подальшої нормотворчої діяльності, пов’язаної із удосконаленням вітчизняного кримінального законодавства.

Загальні ознаки, система й види військових злочинів передбачені у розділі XIX Особливої частини КК України.

Звідси до істотних ознак указаних злочинів відносяться:

1) їх об’єкт (установлений порядок несення чи проходження військової служби) та

2) їх спеціальний суб’єкт, яким є військовослужбовці Збройних Сил України та інших державних органів, перелік яких надано у ч. 2 ст. 401 КК України [2, с. 917].

Систему військових злочинів та їх видів та відповідальності за них складають 34 статті (ст. 401 – 435) КК України. Залежно від безпосереднього об’єкта, на які посягають військові злочини, на думку таких науковців, як Анісімов Г.М., Дзюба Ю.П. та Касинюк В.І., можна виділити такі їх групи:

І. Злочини проти порядку підлеглості та військової гідності: непокора (ст. 402), невиконання наказу (ст. 403), опір начальникові або примушування його до порушення службових обов’язків (ст. 404), погроза або насильство щодо начальника (ст. 405), порушення статутних правил взаємовідносин між військовослужбовцями за відсутності відносин підлеглості (ст. 406 КК України).

II. Злочини проти порядку проходження військової служби: самовільне залишення військової частини або місця служби (ст. 407), дезертирство (ст. 408), ухилення від військової служби шляхом самокалічення або іншим способом (ст. 409 КК України).

III. Злочини проти порядку збереження та користування військовим майном: викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових або інших бойових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства або зловживання службовим становищем (ст. 410), умисне знищення або пошкодження військового майна (ст. 411), необережне знищення або пошкодження військового майна (ст. 412), втрата військового майна (ст. 413 КК України).

IV. Злочини проти порядку експлуатації військової техніки: порушення правил поводження зі зброєю, а також із речовинами і предметами, що становлять підвищену небезпеку для оточення (ст. 414), порушення правил водіння або експлуатації машин (ст. 415), порушення правил польотів або підготовки до них (ст. 416), порушення правил кораблеводіння (ст. 417 КК України).

V. Злочини проти порядку несення бойового чергування та інших спеціальних служб: порушення статутних правил вартової служби чи патрулювання (ст. 418), порушення правил несення прикордонної служби (ст. 419), порушення правил несення бойового чергування (ст. 420), порушення статутних правил внутрішньої служби (ст. 421 КК України).

VI. Злочини у сфері охорони державної таємниці: розголошення відомостей військового характеру, що становлять державну таємницю, або втрата документів чи матеріалів, що містять такі відомості (ст. 422 КК України).

VII. Військові службові злочини: недбале ставлення до військової служби (ст. 425), бездіяльність військової влади (ст. 426 КК України).

VIII. Злочини проти порядку несення військової служби на полі бою та в районі бойових дій: здача або залишення ворогові засобів ведення війни (ст. 427), залишення гинучого військового корабля (ст. 428), самовільне залишення поля бою або відмова діяти зброєю (ст. 429), добровільна здача в полон (ст. 430), злочинні дії військовослужбовця, який перебуває в полоні (ст. 431), мародерство (ст. 432 КК України).

IX. Злочини, відповідальність за які передбачена міжнародними конвенціями та договорами: насильство над населенням у районі воєнних дій (ст. 433), погане поводження з військовополоненими (ст. 434), незаконне використання символіки Червоного Хреста, Червоного Півмісяця, Червоного Кристала та зловживання ними (ст. 435 КК України) [3, с. 20-21]. Ми вважаємо, що такий поділ військових злочинів на групи є доцільним, оскільки до уваги береться безпосередній об’єкт, на який посягають такі злочини.

Чинний Кримінальний кодекс України зберіг в Особливій частині окремий розділ XIX “Злочини проти встановленого порядку несення військової служби (військові злочини)”, яким передбачається відповідальність за вчинення військових злочинів. Аналіз практики застосування статей розділу XIX КК України свідчить про наявність багатьох проблем, які виникають у правозастосовчих органів. Проблемними та такими, що потребують наукових досліджень, залишаються питання щодо відмежування військових злочинів від суміжних з ними злочинів [4].

Згідно ч. 1 статті 401 КК України військовими злочинами визнаються передбачені цим розділом (розділом XIX) злочини проти встановленого законодавством порядку несення або проходження військової служби, вчинені військовослужбовцями, а також

військовозобов’язаними під час проходження ними навчальних (чи перевірних) або спеціальних зборів.

Як зазначають М.І. Панов, Н.О. Гуторова, родові поняття окремих груп злочинів, передбачених у розділах Особливої частини КК України, є поняттями доктринальними. Вони виступають науковими логіко-юридичними абстракціями, які виконують важливу функцію засобів наукового пізнання соціально-правових явищ. Винятком є закріплення в законі родового поняття злочинів проти встановленого порядку несення військової служби (військові злочини) [5, с. 296].

З огляду на юридичне визначення поняття військового злочину, передбаченого ст. 401 КК України, суб'єкти злочину, передбачені у розділі XIX КК України, особи, що не мають статусу військового та не несуть службу, тобто цивільні, не можуть бути визнані винними у вчиненні злочину (за винятком співучасті) [6, с. 113]. Проте реальність сучасності, тенденція до збільшення кримінальних правопорушень у військових формуваннях держави, вчинені цією конкретною категорією осіб, тяжкість наслідків таких правопорушень, що несуть суспільну небезпеку вимагає проведення наукового дослідження щодо доцільності законодавчого перегляду положень цієї статті та внесення можливих змін у неї.

В останні роки на етапах реформування Збройних Сил України та інших державних військових формувань, сформованих відповідно до законів України, для значної кількості посад, що раніше займали лише військовослужбовці, стало можливим замінити їх цивільними особами. Також не було винятком, коли діяльність посадових осіб є вирішальною для бойової готовності державних військових формувань та здатності виконувати свої конституційні завдання та функції. Статистичні дані показують, що цивільні особи, які займають такі посади у таких військових формуваннях, вчиняють різні види злочинів, в тому числі тяжкі та особливо тяжкі. Така статистика є додатковим аргументом на користь позиції щодо необхідності проведення досліджень щодо доцільності законодавчого перегляду положень ст. 401 КК України.

Окрім проблем застосування кримінально-правових норм щодо вчинених злочинних діянь, що відносяться до розділу в цілому, існує ряд проблем щодо кваліфікації також окремих злочинів, передбачених цим розділом. Аналіз результатів правоохоронних органів, а також теоретичних досліджень вказують на недосконаліть деяких статей у цьому розділі, що також піднімає ці проблеми. Таким чином, однією з таких є ст. 410 КК України “Викрадення, привласнення, вимагання військовослужбовцем зброї, бойових припасів, вибухових або інших бойових речовин, засобів пересування, військової та спеціальної техніки чи іншого військового майна, а також заволодіння ними шляхом шахрайства або зловживання службовим становищем”. Також проблемою є те, що при застосуванні цієї статті в деяких випадках можна виявити недосконаліть законодавчої структури та щодо вказівки на предмет злочину. Таким чином, ч. 3 ст. 410 КК України передбачає відповідальність за вчинення пограбування з метою захоплення тільки зброєю, військовими запасами, вибуховими та іншими військовими речовинами, засобами транспорту, військовими та спеціальними засобами. При цьому за жорстоке поводження з метою окупації іншого військового майна відповідальність не встановлена.

Висновки.

В умовах глобалізації злочинності кримінальне право України може та повинно бути гармонізованим і з міжнародним правом. Цього вимагають умови сучасного взаємопов’язаного та взаємозалежного світу.

Ефективність боротьби проти злочинності залежить від багатьох факторів. Одним із таких чинників є правильність кримінально-правової оцінки суспільно-небезпечних діянь, вчинених у військовій сфері. З огляду на це пропонується Розділ XX Кримінального кодексу України “Злочини проти миру, безпеки людства та міжнародного правопорядку” перейменувати на “Злочини проти миру, людяності та військові злочини”, а розділ XIX “Злочини проти встановленого порядку несення військової служби (військові злочини)” – на “Злочини проти встановленого порядку несення військової служби”.

Таким чином, проголошення в Україні незалежності, реалізація на практиці положень Конституції України щодо захисту прав, свобод, законних інтересів людини і громадянина, а також спрямованість її на вступ до Європейського Союзу поставили перед вітчизняною юридичною наукою принципово нові фундаментальні питання. Тому слід переглянути відповідне військове законодавство.

Використана література

1. Сарнавський О.М. Норми про кримінальну відповідальність військово-службовців у системі кримінального права України // Часопис Київського університету права. – 2013. – № 2. – С. 308–311.

2. Кримінальний кодекс України . науково- практичний коментар : у 2 т. – Т. 2 : Особлива частина / [Ю.В. Баулін, В.І. Борисов, В.І. Тютюгін та ін.]. – [5-те вид., допов.]. – Х. : Право, 2013. – 1040 с.

3. Злочини проти встановленого порядку несення військової служби (військові злочини) : навч. посіб. / [Г.М. Анісімов, Ю.П. Дзюба, В.І. Касинюк та ін.] ; за ред. М.І. Панова. – Х. : Право, 2011. – 184 с.

4. Черниш О.В. Питання кримінально-правової кваліфікації у військовій сфері : матеріали конференцій. – (Репозитарій Національного Авіаційного Університету). – Режим доступу : http://www.er.nau. edu.ua/ handle/NAU/27643

5. Панов М.І., Гуторова Н.О. Методологічні засади дослідження проблем Особливої частини кримінального права // Вісник Академії правових наук України. – 2009. – № 100. – С. 291-304.

6. Колодяжний М. Г. Кримінологічна характеристика військових злочинів в Україні // Питання боротьби зі злочинністю : зб. наук. пр. – Харків. : Право, 2013. – Вип. 26. – С. 109-117.

Рецензент статті: Катеринчук К.В., *к.ю.н., доцент.* Доцент кафедри кримінального права і процесу Навчально-наукового Юридичного інституту.

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

УДК 343.412:179.7(045)

ГУЦАЛ І.Ю., студентка Навчально-наукового Юридичного інституту
Національного авіаційного університету

ПИТАННЯ ЛЕГАЛІЗАЦІЇ ЕВТАНАЗІЇ В УКРАЇНІ: ІНОЗЕМНИЙ ДОСВІД

Анотація. *Стаття присвячена питанню доцільності легалізації евтаназії в Україні. На прикладі країн Європи та Америки було здійснено аналіз явища евтаназії, його впливу на законодавство та суспільство. Автор зазначає особливості проведення евтаназії в кожній проаналізованій країні. Як висновок, автор обгрунтовує неоднозначність зазначеного питання та звертає увагу на ризики, які можуть виникнути у результаті легалізації евтаназії в Україні.*

Ключові слова: *евтаназія, активна евтаназія, пасивна евтаназія, суспільство, закон, легалізація.*

Summary. *This article is devoted to the issue of euthanasia legalization expediency in Ukraine. On the example of countries in Europe and America, an analysis was made of the phenomenon of euthanasia, its impact on legislation and society. The author highlights the peculiarities of euthanasia in each analyzed country. As a conclusion, the author substantiates the ambiguity of this issue and draws attention to the risks that may arise as a result of the legalization of euthanasia in Ukraine.*

Keywords: *euthanasia, active euthanasia, passive euthanasia, society, law, legalization.*

Аннотация. *Статья посвящена вопросу о целесообразности легализации эвтаназии в Украине. На примере стран Европы и Америки был проведён анализ явления эвтаназии, его влияния на законодательство и общество. Автор отмечает особенности проведения эвтаназии в каждой проанализированной стране. Как итог, автор обосновывает неоднозначность указанного вопроса и обращает внимание на риски, которые могут возникнуть в результате легализации эвтаназии в Украине.*

Ключевые слова: *эвтаназия, активная эвтаназия, пассивная эвтаназия, общество, закон, легализация.*

Постановка проблеми. Відповідно до Конституції України та міжнародних договорів, ратифікованих Верховною Радою України, найважливішим природним правом людини є її право на життя. Відповідно до ст. 3 Конституції України людина, її життя і здоров’я, честь і гідність, недоторканність і безпека визнаються найвищою соціальною цінністю [1]. Саме тому у нашій державі евтаназія є кримінально-караним діянням. Такий склад злочину, поки що, не регламентований Кримінальним Кодексом України, але теорія кримінального права визначає, що добровільна згода людини на позбавлення її життя не виключає карності діяння і, як правило, кваліфікується за ст.115 КК України як умисне вбивство [2]. Хоча, в деяких сучасних країнах світу дане явище вважається нормою і давно легалізоване на законодавчому рівні. Порівняльний аналіз показників, які стосуються наслідків евтаназії в країнах, де вона легалізована дасть змогу зробити висновок щодо доцільності регламентації даного явища в Україні.

Результати аналізу наукових публікацій. Питання евтаназії досліджується не лише юристами, а і медиками, філософами, соціологами. Дане явище було предметом дослідження таких науковців, як А. Пронін, Р. Стефанчук, О. Пунда, О. Олейник, Д. Мельников, Л. Черна, А. Сухолуцкий, Б. Ентин, Т. Самсонова , Н. Жукова, М. Ткач та інші.

Метою статті є аналіз розвитку явища евтаназії у деяких іноземних державах та доцільності реалізації в Україні практики припинення лікарем життя людини, яка має невиліковне захворювання, на задоволення її прохання в безболісній або мінімально болісній формі припинити страждання в Україні.

Виклад основного матеріалу. У наш час термін “евтаназія” дедалі частіше зустрічається не тільки у професійному спілкуванні лікарів, юристів, політиків, а й у дискусіях звичайних пересічних громадян. Загалом під евтаназією розглядають практику припинення (або скорочення) лікарем життя людини, яка страждає на невиліковне захворювання, відчуває нестерпні страждання, на задоволення прохання хворого в безболісній або мінімально болісній формі з метою припинення страждань [3]. Даний термін використовується уже давно. Його запровадив англійський філософ Френсіс Бекон ще у сімнадцятому столітті. “Евтаназія” – в перекладі з грецької, означає “добра смерть”, проте, як свідчать історичні факти, це не завжди було так.

Ще в давній Спарті подібним способом позбавляли життя слабких та хворих немовлят. В племенах з первіснообщинним ладом вбивали людей літнього віку, які ставали кволими та були тягарем для нового покоління. Сумний досвід зловживання евтаназією в фашистській Німеччині змушує і сьогодні не тільки німців, але й увесь світ здригатися при згадці про звірства, вчинені під маскою гуманізму [4, с. 186]. Проте, навіть беручи до уваги подібний негативний досвід наших попередників, дане явище знаходить багато прихильників у сучасному світі.

Розрізняють два основні види евтаназії: пасивна евтаназія (умисне припинення лікарем терапії, яка підтримує життєдіяльність пацієнта), активна евтаназія (введення смертельно хворому медичних препаратів, або інші дії, які тягнуть за собою швидку та безболісну смерть). До активної евтаназії часто відносять і самогубство з лікарською допомогою.

Насправді актуальним питання евтаназії стало лише у XX столітті. Саме тоді було здійснено перший досвід її легалізації, а також практичного викристання всупереч чинному законодавству.

Упродовж XX століття пасивна евтаназія використовувалась у більшості країн світу. За результатами соціологічних досліджень 1998 року, що були опубліковані в Міжнародному медичному журналі, 40 % смертей тяжкохворих припадає на факти застосування пасивної евтаназії. Пацієнти помирали “за попередньою домовленістю” з медиками або внаслідок офіційної відмови в лікуванні, або за допомогою ліків, що прискорювали летальний кінець [5].

Розвиток активної евтаназії відбувався дещо іншом чином. Умертвіння хворого зі співчуття дозволялось ще Кримінальним кодексом Радянської Росії 1922 р. Проте, з часом таке право було скасовано. Евтаназію, зазвичай, застосовували у концтаборах для масового знищення євреїв, які через важкі хвороби не могли виконувати свою роботу. Міжнародний військовий трибунал у Нюрнберзі кваліфікував дії таких “лікарів” як злочин проти людства.

Після Другої світової війни евтаназія була легалізована тільки у 1977 р., коли в США (Каліфорнія) було ухвалено перший в світі закон “Про право людини на смерть”, згідно з яким було дозволено здійснення пасивної евтаназії. Сумнозвісний приклад доктора Джека Кеворкяна із США (“Доктор смерть”), якого шість разів засуджували до ув’язнення за використання активної евтаназії для 130 осіб і стільки ж разів виправдовували, поступово перетворився у феномен соціального замовлення смерті [6, с. 8].

Наразі практика застосування евтаназії поширена у багатьох країнах світу. Яскравим прикладом є Нідерланди. Після довгих ваганнь і переговорів у цій країні евтаназію легалізували на законодавчому рівні у 2002 р. Крім того, допомога у скоєнні самогубства у Нідерландах теж не карається законом.

При цьому для проведення евтаназії необхідне дотримання основних вимог: пацієнт повинен бути невиліковно хворим, страждати від “нестерпного” болю та не мати ніякого шансу на одужання. Така особа повинна бажати настання своєї смерті, знаходячись при здоровому розумі і наполягати на цьому протягом певного періоду часу.

Дане явище вже декілька років поспіль вдало регулюється чиним законодавством Нідерландів і єдиним спірним питанням в даній сфері досі є вік, з якого можна застосовувати евтаназію. Наразі допустимим віком визначено 12 років (за згодою батьків).

Швейцарія також є країною, в якій право на смерть закріплене на законодавчому рівні. Сьогодні на швейцарських сайтах, в мережі Інтернет, можна придбати путівку з метою евтаназії в один кінець. Згідно із місцевим законодавством, надання допомоги в акті самогубства за умов відсутності особистих корисних цілей не забороняється. З такою метою сюди приїжджають іноземці, оскільки це єдина країна світу, де евтаназія дозволяється для жителів інших країн [7]. В деяких країнах сучасної Європи, де евтаназія заборонена, існує офіційний алгоритм її здійснення: маючи довідки, які засвідчують наявність невиліковної хвороби у пацієнта та бажання даної особи покинути цей світ, він може звернутися до лікаря за направленням до Швейцарії для проведення, безпосередньо, евтаназії.

Бельгія, країна, яка за прикладом Нідерландів прийняла закон, що легалізував евтаназію на території цієї держави, ще в 2002 р. Відповідно до закону Бельгії “Про евтаназію” її може провести виключно лікар, який тривалий час веде нагляд за невилковно хворим. Пацієнтами можуть бути тільки громадяни Бельгії, які постійно проживають в країні. Для уникнення зловживань, пов’язаних з проведенням асистованої смерті, в державі створена спеціальна комісія, яка розглядає всі випадки та уповноважена встановлювати, що медичні працівники не порушували законодавство. У 2014 році Король Бельгії підписав законопроект, який дозволяє дитячу евтаназію [9]. У 2016 році був зафіксований перший випадок застосування евтаназії до неповнолітнього.

В цілому, в США евтаназія є забороненною. Питання про те, дозволити чи ні допомогу у звершенні самогубства, було винесено на розгляд у окремих штатах. Тільки у трьох штатах США (Орегон, Вашингтон, Вермонт) легалізована активна евтаназія, але за умов, якщо смертельну ін’єкцію здійснює сам пацієнт (або випиває відповідні ліки з дозволу лікаря). Четвертий штат, де також застосовується евтаназія, проте зі значними обмеженнями – Монтана [8]. Орегон у 1997 р. став першим штатом, який дозволив допомогу у звершенні самогубства, прийнявши закон під назвою “Смерть з гідністю”. Законодавці Нью-Мексико скасували рішення Верховного Суду штату, який дозволяв евтаназію, і наразі цей законопроект перебуває на юридичній експертизі.

З 2009 року евтаназія, як активна, так і пасивна стала дозволена і в Люксембурзі. Законодавство щодо цього питання схоже на те, що і у Бельгії, в ньому підкреслюється “право лікарів на свободу совісті”.

У 2015 році, до країн, які легалізували право на смерть, приєдналась і Німеччина. Бундестаг уже давно мав намір узаконити евтаназію, проте чи не єдиним чинником, який загальмував цей процесс, було історичне минуле цієї країни. Даним законом дозволена виключно пасивна евтаназія, активна досі залишається забороненою та тягне за собою кримінальну відповідальність.

Законодавство усіх цих країн щодо питання евтаназії дуже детально розроблене, проте навіть за цієї умови деякі законні процедури часто призводять до зловживань. Наприклад, у Великій Британії у 2007 році було законодавчо затверджено акт про Ментальні здібності, згідно з яким, якщо пацієнт втрачає стан здорового мислення або знаходиться у несвідомому стані, він може заздалегідь призначити собі представника, який має змогу написати заяву про пасивну евтаназію для нього. Цей акт надав можливість для відкриття нового виду бізнесу. Одна з таких організацій – “Співчуття у смерті”, що допомагає парам похилого віку оформити відповідні документи один на одного. Таке право дається не тільки родичам, а і співмешканцям, не зареєстрованим у шлюбі законодавчо, тому ця фірма використовує вираз: “той, кого ви кохаєте і той, хто кохає вас”. Норма прибутків цієї компанії складає 70 %, а це свідчить, що оформлення права на евтаназію – прибутковий бізнес [8]. Звичайно, за таких умов, заохотивши як можна більше клієнтів, фірма примножує свої прибутки. Зловживання даною нормою можливі також і з боку родичів чи співмешканців у корисливих цілях.

На початку нашого дослідження ми зазначали, що в Україні евтаназія суворо заборонена. З юридичної точки зору, відповідно до сучасного українського законодавства, евтаназія досі прирівнюється до самогубства чи умисного вбивства, яке карається позбавленням волі на строк від семи до п’ятнадцяти років [2]. Також в ч. 3 ст. 52 Основи законодавства України про охорону здоров’я мова йде про те, що медичним працівникам забороняється здійснення евтаназії, навмисного прискорення смерті або умертвіння невиліковно хворого з метою припинення його страждань [10].

Звичайно, в Україні, як і в багатьох інших цивілізованих країнах світу були спроби частково узаконити евтаназію. Проте жодна з цих спроб не закінчилась безпосередньо її легалізацією. Пригадаємо, що у процесі підготовки Цивільного кодексу України у 2003 році було здійснено спробу легалізації добровільної пасивної евтаназії у нашій країні. Однак, в остаточному варіанті дана пропозиція не знайшла свого відображення; за неофіційними даними, найвагомішим аргументом проти евтаназії у той час стала можливість лікарської помилки.

З точки зору медиків, більшість українських лікарів однозначно відкидають евтаназію, вважаючи дану практику морально неприпустимою. Хоча невідомо, чи справді ці лікарі розуміють суть даної проблеми. Особливо негативно ставляться до евтаназії лікарі анестезіологи та реаніматологи. Лікарі-реаніматологи роблять усе можливе для порятунку людського життя. Вони заявляють, що борються за життя людини до моменту настання смерті головного мозку, коли зрозуміло, що врятувати пацієнта неможливо – лише тоді приймають остаточне рішення припинити спроби порятунку.

Лікарі також зазначають, що рівень розвитку медицини ніколи не стоїть на місці. Він постійно удосконалюється, що може дати змогу лікарям рятувати так званих невиліковних на сьогодні хворих. Запровадження евтаназії може пригальмувати цей розвиток, адже ні у лікарів, ні у хворих не буде мотивації продовжувати лікування, використовуючи дедалі новіші методи. Також, слід зазначити, що у випадку, коли евтаназію проводить лікар, це є грубим порушенням клятви Гіппократа, а саме положення: “я не дам нікому просимого у мене смертельного засобу і не покажу шляху для подібного замислу”.

Серед українських лікарів є і прихильники евтаназії. Частина лікарів поділяє думку, що людина за своєю волею може відходити з життя, якщо таке право вибору буде прийняте медичною спільнотою. Вони запевняють, що при вирішенні подібного питання обов’язковою є участь психіатра. Лікарі наголошують, що у випадку вибору

добровільної смерті до кожного пацієнта потрібен індивідуальний підхід, зважаючи на психічний та фізичний стан такого пацієнта.

Як бачимо, серед лікарів є як прихильники легалізації даного явища в нашій державі, так і ті, хто її не підтримує.

З точки зору звичайних пересічних громадян, також є певні протиріччя. Противники мотивують свою думку морально-етичними та релігійними переконаннями. Маємо зазначити, що більшості прихильників евтаназії важко обгрунтувати своє позитивне ставлення до неї. На нашу думку, найвагомішим поясненням прихильників є те, що вони знаходяться під впливом своїх матеріалістичних поглядів на життя і переконані, що доки людина дієздатна, вона потрібна суспільству, а невиліковно хворі створюють так звані “труднощі” різного характеру і евтаназія необхідна, щоб уникнути цих труднощів.

Спираючись на вищезазначене, питання щодо доцільності легалізації евтаназії в Україні є неоднозначним. Ми спостерігаємо дві протилежні точки зору, що утворились у суспільній думці: прихильників і противників легкої смерті. Перші переконані, що евтаназія є “гідним виходом з життя”, у той час, як інші будь-який вид евтаназії сприймають не інакше як вбивство чи самогубство. Проте, якщо лікар легально буде здатний вбити людину, реалізовуючи її право на смерть, чи не породить таке право низку нових проблем, ще страшніших та глобальніших?

Висновки.

Проаналізувавши досвід іноземних держав, які на законодавчому рівні уже закріпили евтаназію, спостерігаємо певні тенденції.

По-перше, до легалізації легкої смерті законодавство цих країн мало певне нормативне підгрунття або історичні передумови.

По-друге, суспільство даних держав переважно позитивно ставиться до даного явища і це вже унормовано.

По-третє, у наведених країнах питання щодо евтаназії регулюються чіткими, деталізованими нормативно-правовими актами та створюються спеціальні служби та комісії до компетенції яких відносяться виключно питання, пов’язані з евтаназією.

Таким чином, спираючись на іноземний досвід, варто все ж визнати, що ні українське законодавство, ні українське суспільство поки що не готові до такого великого кроку, як легалізація евтаназії. Дана проблема в Україні потребує, насамперед, кримінально-правової регламентації. Від вирішення цієї проблеми залежить доля великої кількості безнадійно хворих людей, які останні роки перебувають у лікарнях, фізичний стан яких діагностується як проміжний – між життям та смертю, а психічний – це безпорадність та стан глибокого відчаю. На даний момент питання евтаназії є неоднозначним і не має достатнього підґрунтя для легалізації в Україні, але це лише питання часу. З удосконаленням і демократизацією правової системи цілком можливо, що законодавець закріпить право на життя і смерть. Легалізація евтаназії повинна пройти низку наукових, законодавчих фільтрів, які встановлять правила, конкретні критерії та випадки, коли таке право може бути реалізоване. Право на життя є основним правом людини, від якого залежить реалізація інших прав, тому актуальність розгляду данного питання і його обговорення є досить нагальним в сучасних умовах в Україні.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР : за станом на 13.09.16 р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/254к/96-ВР

2. Кримінальний кодекс України : Закон україни від 5.04.01 р. № 2341-ІІІ : за станом на 13.07.17 р. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/2341-14

3. Олейник О. Этические и правовые аспекты эвтаназии // Юридична прктика – 2001. – № 48. – (28 ноября).

4. Мельников Д. Тайны гестапо. Империя смерти / Д. Мельников, Л. Черна. – М. : Вече, 2000. – 480 с.

5. Безаров О.Т. Евтаназія в контексті медичної практики (за результатами соціологічного опитування, проведеного в м. Чернівці) // Буковинський медичний вісник. – 2005. – № 1. – С. 149-154. – Режим доступу: http://tanat.info/eutanazija-v-konteksti-medichnoi-praktiki-24-12-2013.html

6. Тимощук О. Наслідки евтаназії, або чи узаконять добровільну смерть в Україні? / “Дзеркало тижня. Україна”. – № 48. – (20 грудня 2013 р.) – Режим доступу : http://gazeta.dt.ua/family/naslidki-evtanaziyi-abo-chi-uzakonyat-dobrovilnu-smert-vukrayini-_.html

7. Сухолуцкий А., Ентин Б., Самсонова Т., Жукова Н. Как относятся к эвтаназии в других странах? – (14 октября 2013 года). – Режим доступу : http://www.echo.msk.ru/blog/roadmap/1176606-echo

8. Ткач М.Є. Філософське осмислення евтаназії в умовах сучасного суспільства. – Режим доступу : http://s-journal.cdu.edu.ua/base/2008/v4/v4pp209-211.pdf

9. Эвтаназия в Бельгии. – Режим доступу : https://evtanazija.ru/belgiya

10. Основи законодавства України про охорону здоров’я : Закон України. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2801-12

Рецензент статті: Катеринчук К.В., *к.ю.н., доцент.* Доцент кафедри кримінального права і процесу Навчально-наукового Юридичного інституту.

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

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 доктора і кандидата юридичних 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 пояснювати наукове вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:

інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   – *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   – *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   – *відстань між рядками – 1 інтервал;*
   – *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов’язкові структурні елементи:
   - УДК.
   - Ім’я та прізвище, науковий ступінь, вчене звання автора, місце роботи.
   - Назва статті.
   - Анотація та ключові слова – укр., англ., рос. мовами.
   - **Розв’язання проблеми,** шляхом наукового вирішення завдання:
     - **постановка проблеми** *(загальна характеристика)* та **результати аналізу наукових публікацій** *(досліджень)*, в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;
     - **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** *(згідно з наказом ВАК України від 26.01.08 р. № 63).*
   - 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 наукових результатів.***
   - ***Наукова (практична) цінність результатів.***
   - ***Заключення про можливість відкритої публікації.***

3) Рукопис статті та Відгук мають бути ретельно вичитаними, виправленими і підписаними відповідними особами.

4) Окремим файлом автори подають електронну версію **розширеної анотації статті** (до 1 сторінки формату А-4) **англійською мовою,** яка буде розміщена на веб-сторінці журналу, відповідно до наказу Монмолодьспорту України “Про затвердження порядку формування переліку наукових фахових видань України” від 17.10.12 р. № 1111.

5) За надання послуг щодо розгляду, форматування, корегування, тиражування та ін. робіт, пов’язаних з публікацією статей та виданням журналу, **пропонується здійснити оплату в розмірі 280 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.

Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Редакційна колегія не завжди поділяє погляди авторів публікацій.
  Статті видаються в авторській редакції.
  Відповідальність за достовірність інформації, що міститься в статтях і повідомленнях журналу, лежить на їх авторах.
- 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 зі скороченням обсягу матеріалу.

* * * * * * * * * *

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 4(23)

2017

Засновники журналу:	- 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”.
Видавець:	© Науково-дослідний інститут інформатики і права Національної академії правових наук України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. НДІ інформатики і права НАПрН України. Тел.: 234-94-56, e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	//www.ippi.org.ua – НДІ інформатики і права НАПрН України; //www.nbuv.gov.ua – Нац. бібліотека України ім. В.І. Вернадського.