Науково-дослідний інститут інформатики і права
Національної академії правових наук України

Національна бібліотека України ім. В.І. Вернадського
Національної академії наук України

Відкритий міжнародний університет розвитку людини "Україна"

ISSN 2616-6798

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 3(26)/

2018

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

Згідно з Наказом МОН України від 11.07.16 р. № 820 (додаток 12)
у журналі можуть публікуватися матеріали стосовно дисертаційних робіт
на здобуття наукових ступенів доктора і кандидата наук у галузі юридичних наук.
Друковане періодичне видання "Інформація і право" внесене в міжнародну базу даних
періодичних видань, згідно відповідного номеру ISSN

м. Київ

Research Institute of informatics and rights of National academy of legal sciences of Ukraine

Vernadsky National Library of Ukraine of National academy of sciences of Ukraine

Open International University of Human Development “Ukraine”

ISSN 2616-6798

INFORMATION AND RIGHT

SCIENTIFIC PROFESSIONAL MAGAZINE

№ 3(26)/

2018

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

Pursuant to Order of Department of education of Ukraine dated 11.07.16 № 820 (addition 12) materials can be published in a magazine related to dissertation works aimed on the receipt of scientific degrees of doctor and candidate of sciences in the area of legal sciences

Kyiv

УДК 002:340+316.4+338.46

* * * * * * * * * * *

UDC 002:340+316.4+338.46

* * * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

Інформація в інших галузях права

До відома читачів

Наукове редагування, створення оригінал-макета та дизайн – Брижко В.М.
Граматичне коректування – Майстренко І.А. (укр., англ.).
Формат 70 х 108/16. Спосіб друку – різографія. Ум. друк. арк. 12.3. 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 26.09.18 р.

TABLE OF CONTENTS

Informative right

Legal informatics

Informative and national safety

Information in other fields of rights

Recommended for publication by the Academic Board of Institute of informatics and right of National academy of legal sciences of Ukraine, protocol № 8 dated 26.09.18

Інформаційне право

УДК 342.9

ПАНОВА І.В., *кандидат юридичних наук, доцент*, доцент кафедри загальноправових дисциплін факультету № 6 ХНУВС

ФАКТОРИ, ЩО ВПЛИВАЮТЬ НА УТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ПРАВА ТА ФОРМУВАННЯ ЇЇ ЗМІСТУ

Анотація. *В цій статті сформульовано місце інформаційного права в системі права України, виконано дослідження наукових поглядів на проблему визначення системи інформаційного права, охарактеризовано її складові елементи, розкрито фактори, що впливають на утворення системи інформаційного права та формування її змісту та означено тенденції розвитку науки інформаційного права України на сучасному етапі.*

Ключові слова: *інформаційне право, система інформаційного права, норма інформаційного права, інститут інформаційного права, галузь інформаційного права.*

Summary. *This article describes the place of information law in the system of law of Ukraine, researches the scientific views on the problem of determining the system of information law, describes its constituent elements, discloses the factors that influence the formation of the information law system and the formation of its content, as well as the trends of the development of information law science in Ukraine at the present stage.*

Keywords: *information law, system of information law, norm of information law, institute of information law, sphere of information law.*

Аннотация. *В этой статье сформулировано место информационного права в системе права Украины, выполнено исследование научных взглядов на проблему определения системы информационного права, охарактеризованы ее составляющие элементы, раскрыто факторы, влияющие на возникновение системы информационного права и формирования его содержания и отмечено тенденции развития науки информационного права Украины на современном этапе.*

Ключевые слова: *информационное право, система информационного права, норма информационного права, институт информационного права, отрасль информационного права.*

Постановка проблеми. Постійне збільшення ролі інформації в суспільних відносинах можна назвати однією з предметних властивостей сучасного світового соціального прогресу, в якому стрімко зростає роль права як головного механізму регулювання таких відносин. Однак інформаційне суспільство розвивається такими швидкими темпами, що право суттєво відстає від його потреб, і саме тому в інформаційній сфері постійно виникає проблема взаємоузгодженості системоутворюючих елементів інформаційного права, до того ж між діючими нормативно-правовими актами існують протиріччя, що порушують системність законодавства та не сприяють стабільному й послідовному розвитку даної галузі. Крім того, основні напрямки розвитку та удосконалення інформаційного права в Україні пов’язані із соціально-економічними та політичними реформами, які відбуваються в нашій державі. Разом з тим проходять глибокі процеси перетворення самого змісту інформаційного права, постійне оновлення законодавства та усвідомлення нової ролі правових явищ в житті людини в умовах сучасного інформаційного суспільства.

Українське інформаційне суспільство вимагає від правової системи постійного руху, розробки та запровадження актуальних доктринальних домінант, комплексного правового забезпечення інформаційної сфери.

Результати аналізу наукових публікацій. Теоретичним питанням розвитку інформаційного права присвячено наукові праці як вітчизняних вчених: І. В. Арістової, О.А. Баранова, В.М. Брижка, К.І. Бєлякова, В.Д. Гавловського, І.М. Дороніна, О.О. Золотар, Р.А. Калюжного, А.І. Марущака, А.М. Новицького, В.Г. Пилипчука, В.С. Цимбалюка, М.Я. Швеця та ін., так і зарубіжних вчених: І.Л. Бачило, В.Н. Лопатин, М.А. Федотов та ін. Проте багато правових аспектів цієї проблеми залишаються вивченими не повною мірою, а динамічний стан інформаційного законодавства зумовлює появу нових чинників, що впливають на утворення системи інформаційного права та формування її змісту.

Метою статті є дослідження наукових поглядів на проблему визначення системи інформаційного права, а завданням – сформулювати поняття системи інформаційного права, визначити фактори, що впливають на утворення та формування її змісту.

Її новизна полягає в тому, що вперше надано авторський погляд на питання формулювання чинників, що впливають на утворення системи інформаційного права та означено тенденції формування її змісту на сучасному етапі.

Виклад основного матеріалу. Нинішня система українського інформаційного права у зв’язку із розвитком суспільних відносин зазнає істотних змін, сповнюється новим змістом. Виникають і розвиваються нові правові інститути: е-урядування, е-документообіг, е-торгівля тощо [2, с. 38-44; 3, с. 31]. Також передумовою формування інформаційного права як окремої галузі права вбачають існування інформаційного законодавства [12, с. 234-244; 7, с. 70-78; 16].

Варто підтримати точку зору С.В. Бобровник, яка зазначає що “Значний вплив на розвиток системи законодавства спричиняють процеси, пов’язані зі зміною сфери правового регулювання суспільних відносин. Зміна сфери правового регулювання являє собою процес, у якому стикаються протилежні тенденції – розширення та звуження юридичної регламентації. Вказані напрямки здійснюються різними шляхами, основними з яких в сучасних умовах є поширення правового регулювання на раніше не регламентовані правом сфери соціальної дійсності” [10, с. 53]. Все це знаходить свій вираз передусім у зростанні чисельності нормативно-правових актів, іншими словами – у фактичних перемінах в системі законодавства.

Імовірно, через це при знаходженні місця та утвердженні інформаційного права як науки поміж інших правничих наук в Україні, його ввели поряд з теорією управління, адміністративним і фінансовим правом. Нині інформаційне право розвивається у тісному взаємозв’язку з рядом інших соціальних, гуманітарних та технічних і економічних наук, запозичуючи у них методологічні, теоретичні підходи, понятійний апарат, розуміння сутності суспільних відносин, які визначаються технологічними ознаками їх реалізації [6, с. 77-78].

Як правнича єдність галузь інформаційного права є більш-менш суцільною, самостійною підсистемою правового впорядкування. Її визначальна функція – створити щодо інформаційних правовідносин особливий режим правового регулювання – комплекс властивих за природою і характерних за правничою сутністю правових прийомів і способів. Присутність аналогічного режиму дає перспективу не тільки сполучати норми інформаційного права воєдино, створювати організовану систему, але й індивідуалізувати галузь інформаційного права. Юридичний режим визначає правовий статус суб’єктів права; правові способи здійснення прав і виконання обов’язків та діяльність держави, яка спрямована на гарантування неухильного дотримання

інформаційно-правових норм в реальних інформаційних правовідносинах. Завдяки юридичному режиму реалізується результативний вплив галузі інформаційного права як цілісного явища, так і будь-якої складової інституту або норми.

Структурна будова будь-якої правової системи виглядає так, що всі правові норми, які входять до чинного, позитивного права, утворюють одне ціле (діюче право в цілому), розмежоване за сутністю різних норм на відповідні, взаємозв’язані елементи структури права і законодавства. Поширеною є думка, що базисом такої змістовної структури права і законодавства є чітка сфера суспільних відносин – предмет правового регулювання.

Дефініція “система” застосовується в найрізноманітніших галузях людських знань. З філософської точки зору – це специфічно виокремлена із навколишнього середовища цілісна множина елементів, які поєднуються між собою сукупністю внутрішніх відносин і зв’язків [17, с. 254]. Для формулювання національного права і законодавства в інформаційній сфері зазвичай використовують категорії “система інформаційного права” і “система інформаційного законодавства”. Перше з них закріплює елементи організаційного поділу правових норм галузі інформаційного права, друге – елементи організаційного поділу законодавчих актів, котрі сформувалися в Україні в процесі правового регулювання інформаційних відносин.

Таким чином, система інформаційного права – це внутрішня будова галузі, яка відображає послідовне розміщення елементів, що її утворюють, – інформаційно-правових інститутів і норм, їх єдність і структурний взаємозв’язок (узгодженість). Названі в цьому визначенні ознаки характеризують систему права з внутрішнього боку. Вони вказують на те, які зв’язки існують між її елементами, на яких принципах вона побудована.

Для дослідження факторів, що впливають на формування системи інформаційного права, належить на підготовчому етапі з’ясувати проблему щодо структурних складових і критерії формування її змісту. Під структурою системи в юридичній науці розуміють єдність елементного складу системи і взаємодію складових її елементів. Структура – це засіб зв’язку елементів у системі, які забезпечують її спрямоване функціонування та усталеність (стабільність) [8, с. 240].

Таким чином, до структури системи інформаційного права входять: інформаційно-правова норма, інститут інформаційного права, підгалузі та галузь інформаційного права.

Інформаційно-правова норма – початкова, найменша структурна частина інформаційного права, правило поведінки, що визнане і охороняється державою. Інформаційно-правова норма безпосередньо визначає, оформлює, надає юридичного значення суспільним відносинам в інформаційній сфері і знаходить свій зовнішній вираз у правовому приписі. Варто також додати, що наскільки якісно у законодавстві зафіксовано сутність відповідних суспільних відносин, їх учасників, настільки ця норма буде живучою і здатною врегулювати зазначені відносини. За допомогою свого узагальненого значення інформаційно-правова норма переносить притаманні їй властивості на інші складові системи права. ***Структуризація, впорядкованість, злагодженість, взаємозв’язок і класифікація*** видів інформаційно-правових норм спричинені як структурою інформаційно-правових відносин, так і спрямованістю правотворчого органу на їхнє юридичне вираження та оформлення.

Норми права, з яких складається система права, не можуть функціонувати ізольовано. Вони взаємноузгоджені та цілеспрямовані [8, с. 240]. Організаційна гармонійність системи інформаційного права – це зумовлене існування субординаційних і координаційних відносин між нормами та інститутами інформаційного права, а також несуперечність складових системи. Таким чином, система інформаційного права утворюється різними за змістом та обсягом складовими

елементами, які послідовно з’єднують, розміщують нормативну базу у чіткій функціональній направленості.

Інститут інформаційного права – це певна група юридичних норм, які регулюють суспільні відносини окремого інституту інформаційного права (наприклад, інститут засобів масової інформації, інститут інтелектуальної власності та ін.). Інститут інформаційного права унормовує відокремлену площину, частини, напрями інформаційних правовідносин. Він є складовою частиною однієї або кількох галузей права, характеризується тим, що: регулює вид більш чи менш значущих суспільних відносин; є логічно замкнутою, відокремленою сукупністю норм; функціонує автономно, тобто має можливість здійснювати регулювання суспільних відносин незалежно від інших інститутів права (це не означає, що інститут права не має зв’язків з іншими інститутами права) [17, с. 258-259].

Підгалузь інформаційного права – чітка сукупність (об’єднання) правових інститутів, що формується в межах галузі інформаційного права. Як суцільне явище підгалузь інформаційного права визначає особливе коло відносин в межах сфери правового регулювання галузі інформаційного права, яка відзначається правовим відмежуванням, як, наприклад, комунікативне право [13, с. 36-37].

Утворення спеціальних, за предметним змістом і призначенням, правових норм своєрідно доповнює основну, галузеву диференціацію, але не повинно суперечити їй. Норми комплексних актів можуть носити характер виправданих специфікою винятків із загального правила, але не повинні ігнорувати ці правила чи відміняти їх [15, с. 24 – 27]. Варто також наголосити на інституційному характері галузі інформаційного права. Це проявляється у тому, що така юридична конструкція, як система інформаційно-правових норм, міститься здебільшого в нормативно-правових актах, інших джерелах права, які й надають інформаційному праву чітко виражену інституціональну форму; взаємопов’язаність її як прямими, так і непрямими зв’язками з функціями і діяльністю держави, та її органів – законодавчих, правозастосовних, контрольно-наглядових та ін., незмінність і мобільність її як правового феномену.

Розмежування на підгалузі та інститути є відносним, оскільки інформаційне право, як і право в цілому, є єдиною субстанцією, кожна складова якої невіддільна від інших. Саме тому одна норма може одночасно відноситися до декількох правових інститутів або підгалузей інформаційного права.

Завершує систему структура галузі інформаційного права – відокремлена чисельність норм, спрямованих на унормування суспільних відносин в інформаційній сфері. Галузь інформаційного права є складовою частиною української системи права, що в повній мірі враховує спільні відзнаки правового регулювання відносин в інформаційній сфері.

Науковці слушно стверджують, що наявне достатнє підґрунтя для утворення та становлення галузі інформаційного права. Зокрема, можна погодитись з тим, що “підставою та причиною виникнення будь-яких соціальних регуляторів є наявність, реальне існування об’єктів, з приводу яких виникають певні відносини, формування і реалізація певних видів соціально значимої діяльності” [4, с. 84].

Висновки.

Зазначене вище дозволяє сформулювати фактори, що впливають на утворення системи інформаційного права та формування її змісту:

- Необхідність дотримання принципів законності, пріоритету та захисту інформаційних прав і свобод людини і громадянина, рівності громадян перед законом, вільного одержання, використання, поширення та зберігання будь-якої інформації, не

обмеженої законодавством України, які є характерним ядром інформаційного права. А в деяких випадках і обмеження інформаційних прав громадян у зв’язку з виконанням функцій держави [11, с. 30-33].

- Загрози та складності у зв’язку із розповсюдженням та використанням інформації, які треба певним чином здолати. Оскільки мораль не може взяти на себе обов’язок та відповідальність за врегулювання інформаційних відносин, таким регулятором повинно стати інформаційне право, спрямоване на якісне та ефективне регулювання суспільних відносин, що формуються в ході забезпечення реалізації та захисту прав, свобод і законних інтересів фізичних і юридичних осіб в інформаційній сфері.
- Охорона державою відповідних інформаційно-правових відносин і можливість застосування державного примусу.
- Наявність особливих, притаманних для нашої країни, матеріальних, соціальних, культурних, моральних, національних та інших умов життя суспільства.
- Поява інформаційних загроз людині, суспільству та державі. Виникла необхідність у формулюванні, відокремленні та створенні єдиного та класифікованого правового механізму забезпечення інформаційної безпеки [9, с.136-138; 14, с. 62-64].
- Загальнолюдські потреби – наданням організованості й урегульованості суспільним відносинам в інформаційній сфері оскільки її виникнення, існування і розвиток обумовлені реально існуючою системою інформаційних правовідносин, що дозволяє відносити галузь до значимих порядків соціальної організованості.
- Накопичення нормативного матеріалу і розподіл його за структурними складовими – інститутами та підгалузями інформаційного права. Стає більш помітною тенденція до певної уніфікації структурних елементів системи інформаційного права, рівноцінних за об’ємом, структурою та іншими характеристиками, що дозволяє розширити сферу їх взаємодії, підвищити ефективність регулювання інформаційної сфери. Підвищення змісту та якості правового регулювання, обумовило появу та розвиток міжгалузевих інститутів інформаційного права, як то інформаційна безпека тощо. Це зумовлено комплексним характером правового регулювання, особливостями суб’єктів та об’єкта відповідних правових відносин.

Зазначене дозволяє стверджувати, що інформаційне право становить своєрідну юридичну єдність. Норми інформаційного права об’єднуються в певну систему не за особливим методом або механізмом правового регулювання, а також за окремими специфічними принципами, домінантами, своєрідними способами впливу на правовідносини, що підтверджують наявність окремого юридичного режиму та наділяють норми галузевою специфікою. Притому інформаційно-правові норми вбачалося б можливим розпорошити за іншими галузями (як то адміністративне право або цивільне), проте зарахувати їх тільки до однієї із зазначених галузей неможливо.

Можливість розвитку системи інформаційного права в напрямку від сучасної структури з її міцним зв’язком між інститутами та підгалузями до створення такої системи, в якій початкові структурні конструкції існуватимуть в якості релятивної самостійності. У той же час, проблеми, що випливають із природних вимог подальшого розвитку інформаційного суспільства, визначають ціль правотворчого органу з їх врегулювання та удосконалення.

Для подальшого розвитку інформаційного права для науковців визначальним має стати усвідомлення не тільки перемін у соціальних та політичних умовах сучасного етапу розвитку юридичної науки, а й передусім варто брати до уваги зміни юридичного світосприйняття, бачень та думок відносно сучасного становища інформаційного суспільства.

Дійсно, сьогоднішній етап розвитку інформаційного суспільства неможливо забезпечити в межах адміністративного, або цивільного права передусім завдяки трансформації рівня життя, як то: зміні дозвілля, модернізації побуту, інтернаціональному інформаційному обміну, е-торгівлі, е-освіті, осучасненні виробництва, виготовленню ще більш нових програмних та апаратних засобів. А от же, наступне перетворення інформаційного права України вимагає розробки загальнотеоретичних, доктринальних підвалин інформаційного права.

До того ж розмаїття дефініцій і основ, на яких ґрунтується нині категорія “інформаційне право” можна вважати свідченням того, що юридична наука працює над виробленням єдиного підходу до розуміння сутності “інформаційного права” як галузі права, та виокремлення факторів, які впливають на утворення її системи та формування змісту. Як слушно зазначає І.В. Арістова: “актуалізація теоретичних розробок категорій в межах науки інформаційного права не лише дозволить розвивати інформаційне право як галузь права, але й сприятиме формуванню несуперечливої системи юридичних понять” [1, с. 62]. Адже мета та задача науки – своєчасно підмічати проблеми правозастосування, знаходити та пропонувати спільний концептуальний критерій їх вирішення.

Використана література

1. Арістова І.В. Доктрина інформаційного права України // Публічне та приватне право. – 2017. – № 1. – С. 59-63.

2. Баранов О.А. Інститути інформаційного права // Правова інформатика. – № 3 (11)/2006. – С. 39-45.

3. Баранов О.А. Інтернет речей (IoT) : мета застосування та правові проблеми // Інформація і право. – № 2 (25)/2018. – С. 31-44.

4. Бачило И.Л. Информационное право : учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов ; под ред. акад. РАН Б.Н. Топорнина. – СПб. : Издательство “Юридический центр Пресс”, 2001. – 789 с.

5. Бєляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин : “віртуальні правовідносини” / Lex Portys. – № 2-2016. – С. 47-63.

6. Бобровник С.В. Правове регулювання та розвиток системи законодавства України : тези доповідей і наукових повідомлень науково-практичної конференції [“Правова система України: теорія і практика”]. – К., 1993. – С. 53-54.

7. Брижко В.М. Методологічні та правові засади упорядкування інформаційних відносин : монографія. – К. : ТОВ “ПанТот”, 2009 р. – 418 с.;

також див. : Теорія і практика інформаційного права : методологія кодифікації інформаційного законодавства України / В.М. Брыжко // Правова інформатика. – № 1(37)/2013. – С. 70-78.

8. Загальна теорія держави і права : підручник для студентів 3-14 юридичних спеціальностей вищих навчальних закладів / [М.В. Цвік, В.Д. Ткаченко, Л.Л. Богачова та ін.] ; за ред. М.В. Цвіка, В.Д. Ткаченка, О.В. Петришина. – Харків : Право, 2002. – 432 с.

9. Золотар О.О. Ґенеза суспільних відносин щодо інформаційної безпеки людини // Інформація і право. – № 1(24)/ 2018. – С. 139-148.

10. Інформаційне право України : концептуальні основи формування / [Р.А.Калюжний, В.Д. Гавловський, В.В. Гриценко, В.С. Цимбалюк] : зб. наук. праць / Науковий вісник Дніпропетровського інституту МВС України. – 2001. – № 3. – С. 234-244.

11. Марущак А.І. Обмеження інформаційних прав громадян у зв’язку з виконанням функцій держави : зб. матеріалів наук.-практ. конф. [“Актуальні проблеми управління інформаційною безпекою держави”], (м. Київ, 18 березня 2016 р.). – Т. 2. – С. 30-33.

12. Мицкевич А.В. Система права и система законодательства : развитие научных представлений и законотворчества : сборник статей / Проблемы современного гражданского права : – М. : Городец, 2000. – С. 24-27.

13. Новицький А.М. Щодо питання структуризації інформаційного права як наукової категорії / Актуальні проблеми правознавства. – 2016. – № 4. – С. 34-38.

14. Пилипчук В.Г., Доронін І.М. Право національної безпеки та військове право : теоретичні та прикладні засади становлення і розвитку в Україні // Інформація і право. – № 2(25)/2018. – С. 62-72.

15. Скакун О.Ф. Теорія держави і права : підручник ; [пер. з рос.]. – Харків : Консум, 2001. – 656 с.

16. Цимбалюк В.С. Інформаційне право : концептуальні положення до кодифікації інформаційного законодавства : монографія – К. : Освіта України, 2011. – 426 с.

17. Цимбалюк В.С. Інформаційне право (основи теорії і практики) : монографія. – К. : Освіта України, 2010. – 388 с.

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

УДК 1:340.1:316.324.8

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

ПРАВОВИЙ ЗАХИСТ ТА БЕЗПЕКА ПЕРСОНАЛЬНИХ ДАНИХ: СОЦІАЛЬНИЙ І КОМЕРЦІЙНИЙ АСПЕКТИ

Анотація. *Про основні підходи у принципах і механізмах нового порядку захисту та безпеки персональних даних в європейських правових стандартах та запровадження у національне законодавство універсального критерію захисту даних людини.*

Ключові слова: *інформаційне право, персональні дані, захист та безпека даних, правові стандарти.*

Summary. *About basic approaches in principles and mechanisms of a new order of protection and safety of the personal data in the European legal standards and introduction to the national legislation of universal criterion for the person’s data protection.*

Keywords: *information right, personal data, data protection and safety, legal standards.*

Аннотация. *Об основных подходах в принципах и механизмах нового порядка защиты персональных данных в европейских правовых стандартах и внедрении в национальное законодательство универсального критерия защиты данных человека.*

Ключевые слова: *информационное право, персональные данные, защита и безопасность данных, правовые стандарты.*

Постановка проблеми. Економічна та соціальна інтеграція у функціонуванні внутрішніх та транскордонних ринків, запровадження інформаційних технологій і мереж призвело до збільшення потоків обміну персональними даними між окремими фізичними особами, комерційними та державними структурами, об’єднаннями Європейського Союзу (далі – Союз). Одночасно з тим, що технології прискорюють розвиток економіки, забезпечують надання різних послуг та сприяють підвищенню добробуту, вони активно впливають на істотні зміни у сучасному соціальному житті. Це, перш за все, стосується існуючої проблеми вільного обігу персональних даних в межах Союзу, а також їх передачі у треті країни та міжнародні організації, за умов забезпечення при цьому високого рівня їх захисту та безпеки на законодавчій основі.

Вперше у світі головні міжнародно-правові принципи захисту персональних даних були закріплені Конвенцією Ради Європи “Про захист осіб у зв’язку з автоматизованою обробкою персональних даних” від 28 січня 1981 р. № 108[1] [1, с. 66-72], основною метою якої було створення умов гармонізації національних законодавств в контексті *соціальних аспектів*. Згідно з Конвенцію РЄ № 108 збирання, накопичення, зберігання і поширення персональних даних може здійснюватися лише з дозволу особи, відомості про яку опрацьовуються, шляхом обробки електронних даних. Вказаний акт заклав фундамент узгодженості національних систем захисту персональних даних в країнах світу.

[1] Конвенція Ради Європи від 28 січня 1981 року № 108 та Додатковий протокол до неї від 8 листопада 2001 року / [пер. з англ. В. Брижко, О. Баранов від 2001 р.] : офіційно засвідчено МЗС України від 01.07.02 р. № 72/15-077-1412, ратифіковано Законом України від 06.07.10 р. № 2438-VI .

Через 24 роки, коли Інтернет тільки починав свій розвиток, Європейський Парламент і Рада прийняли Директиву 95/46/ЄС [1, с. 273-293], яка стала ключовим етапом у історії розвитку інформаційно-комунікаційного захисту та безпеки людини. Її головною метою вже було створення умов для гармонізації національних законодавств в контексті *економічних аспектів*.

З часом, у процесах глобалізації та міжнародного трансферту даних, стали проглядатися проблеми, які дедалі визначали появу нових загроз у сфері захисту персональних даних, пов’язаною з поширенням таких новітніх технологій, як “Інтернет речей” [2, с. 85-91], “Хмарні технології” [3, с. 47-59], “Великі Дані” [4, с. 58-63], що надають можливість отримання, несанкціонованої обробки, зберігання і використання значних обсягів даних, та їх конвергенція [4, с. 51-67].

Звичайне збирання, обробка та застосування персональних даних, завдяки можливостям соціальних мереж, користувачами яких є 347 млн. європейців [5] (Міжнародний союз електрозв’язку визначає глобальну чисельність користувачів Інтернету в 3,2 млрд. [6]), може надати багато відомостей про окрему людину, яка добровільно їх розміщує в мережі або з примусу надає. Паспортні дані, адреси і поштові зв’язки, номер телефону і телефонні розмови, родичі, наявність домашних тварин, історії хвороб і лікувань, особисті інтереси і бажання, відомості про пересування, про нерухомість та майновий стан, розмір доходів і податків, кредитні картки, купівельна активність, свідоцтва, довідки, квитанції, анкети прийому на роботу, реєстраційні відомості виборця, різні запити з Інтернету, аж до розміру взуття, можуть інкогніто накопичуватися, аналізуватися, фільтруватися, сортуватися і розміщуватися в невідомому докладному електронному досьє (базах даних) на будь-яку людину. Кожного разу після відвідування веб-сайта залишаються електронні сліди, які стають надбанням інших людей, що може бути використано без відома суб’єкта персональних даних для створення його різностороннього, навіть “викривленого портрета”.

В кращому разі збір та обробка персональних даних служать маркетинговим цілям. Комерсанти прагнуть зробити рекламу ефективною, спрямованою на потрібну аудиторію, а значить – адресною. Їм необхідно мати якомога більше персональних даних: стать, вік, рівень доходів, захоплення та багато ін. – все має значення. Звичайно фірми прагнуть відповідати очікуванням клієнтів і пропонують товари, в яких, як вони вважають, є потреба. Масова розсилка даних (інформації) у вигляді реклами та “спаму”, що нав’язується, активно “процвітає” як в Інтернеті, так і у будь-яких ЗМІ.

З іншої сторони, персональні дані збирають та використовують не лише для проштовхування на ринок якогось продукту, але дуже часто й для вимагання коштів, шахрайства, залякування, шантажу, на шкоду репутації і, взагалі, для маніпулювання свідомістю людини з політичною, економічною, навіть, образливою метою.

Сьогодні новітні технології визначають появу нових, значніших ризиків порушення прав на приватність людини. Яскравим прикладом цього є Інтернет речей, завдяки якому може здійснюватися несанкціоноване програмно-автоматизоване збирання та обмін даними між різнофункціональними пристроями. При цьому відомо, що повністю безпечним цифровий пристрій, підключений через мережу до іншого, неможливо зробити у принципі, а уразливість в одному пристрої може спричинити витік даних з іншого. Й це за тих умов діяльності фірм-розробників технологій, коли вони більше стурбовані питанням вартості пристроїв, функціональності і часу виходу на ринок, ніж захистом та безпекою.

В якості іншого прикладу підвищення незахищеності персональних даних громадян в умовах застосування новітніх технологій, можна вказати на так звані “Хмарні технології” з “хмарними сховищами”. При цих моделях обробки та зберігання даних використовуються численні віддалені в мережі сервери, що надаються в користування клієнтам третьою

стороною. Відомості про користувачів обробляється та зберігається в так званому віртуальному сервері. Маючи певні переваги, модель зберігання містить в собі потенційну загрозу безпеці, особливо коли йдеться про приватну інформацію. Фактично вона може бути доступна будь-яким Інтернет-провайдерам і, далі, будь-яким особам.

Вищенаведене, зокрема, й визначає те, що норми Директиви 95/46/ЄС вже не відповідають задачам ефективного захисту та безпеки персональних даних в Інтернеті. Поєднання пристроїв, послуг і мереж технологій Інтернет речей, Хмарних технологій тощо, які функціонують без участі фізичних осіб, призводить до необхідності створення багаторівневої і багатооб’єктної системи забезпечення інформаційної безпеки, що значно складніше, ніж відома донині мережева безпека [7]. Через це ЄС розпочав створення нової, складної правової бази в даній області, яка охоплювала б всі держави-члени ЄС, а також треті країни, які мають ділові стосунки з країнами ЄС.

Метою статті є визначення та узагальнення основних підходів у новому міжнародному та національному порядку захисту та безпеки персональних даних.

Виклад основних положень. 25 травня 2018 року в законодавстві Європейського Союзу у сфері захисту персональних відбулися найбільші за 2 десятиліття зміни. Вступили в дію нові принципи та правила обробки персональних даних. Вони раніше були затверджені Постановою Європейського Парламенту і Ради (2016 р.) і отримали назву “Пакет захисту даних” (з трьох документів), який визначає умови створення узгодженої нормативно-правової бази в усьому європейському регіоні (див. [8, с. 45-57; 9]).

Головним документом сучасних правових стандартів є Регламент (ЄС) 2016/679 від 27.04.16 р. “Про захист фізичних осіб у зв’язку з обробкою персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС (Загальні Положення про захист даних)” (General Data Protection Regulation) [10; 11, с. 6-106].

Регламент (ЄС) 2016/679 (далі – Регламент) має на меті не просто удосконалення захисту та вільного обігу персональних даних фізичних осіб в межах Союзу, а забезпечення еквівалентного рівня та посилення захисту права всіх громадян ЄС щодо безпеки персональних даних. Основою його вимогою є узгодження законів про недоторканність даних на території ЄС та змін у підходах всіх організацій у всьому регіоні до вирішення проблеми забезпечення обов’язкової конфіденційності відомостей щодо персональних даних. Дотепер компаніям та іншим суб’єктам, що мають справу з персональними даними, доводиться враховувати правила щодо захисту даних 28 різних держав-членів ЄС.

У зв’язку з загальними значними проблемами в упорядкуванні інформаційних відносин, зокрема й в сфері захисту персональних даних, нові принципи та порядок їх забезпечення можуть видатися надто складними, проте вони визначаються серйозними наслідками. Вважаємо, що їх слід враховувати, оскільки вони безпосередньо стосуються будь-яких суб’єктів діяльності, зокрема, й в Україні.

Регламент (ЄС) 2016/679 містить 172 п. Преамбули та 99 статей (102 с.), які визначають 7 основних принципів обробки персональних даних, про які раніше у нас вже йшла мова (див. [10; 11]). Вони, згідно ст. 5 Регламенту, передбачають забезпечення наступного:

- ***“законність, справедливість і прозорість”*** **–** персональні дані мають оброблятися, використовуватися та поширюватися згідно закону, справедливо і прозоро по відношенню до суб’єкта даних. Обробка є законною та справедливою тільки за умови, якщо та тією мірою, якою виконується щонайменше одна з наступних умов:

- суб’єкт даних надав згоду на обробку її або його персональних даних для однієї або декількох конкретних цілей;

- обробка є необхідною для виконання контракту, стороною якого є суб’єкт даних, або для вжиття заходів на запит суб’єкта даних перед укладанням контракту;

- обробка є необхідною для виконання юридичних зобов’язань контролера;
- обробка є необхідною для захисту життєво важливих інтересів суб’єкта даних або іншої фізичної особи;
- обробка є необхідною для виконання завдання в інтересах суспільства або при виконанні службових повноважень, наданих контролеру;
- обробка є необхідною щодо обов’язкових юридичних інтересів контролера або третьої сторони, коли ці інтереси не перекриваються інтересами або основоположними правами та свободами суб’єкта даних, що потребують захисту персональних даних, зокрема якщо суб’єкт даних є дитиною. Цей пункт Регламенту не застосовується до обробки, що здійснюється державними органами при виконанні їх завдань.

Щодо прозорості обробки, то суб’єкт має одержати відомості про особу контролера, мету збору даних, а також бути обізнаний про ризики, захисні заходи та свої права стосовно обробки даних. Будь-яку інформацію про цілі, методи і обсяги обробки персональних даних контролер зобов’язаний висловлювати максимально доступно і простою мовою;

- ***“****обмеження цілей****”*** – персональні дані повинні збиратися лише для конкретних і законних цілей, використовуватися виключно в тих цілях, які заявлені компанією (он-лайн-сервісом) і не піддаватися подальшій обробці, яка несумісна з такими цілями. Якщо із первісної мети випливатиме інша, то згоду має бути дано для обох. Обробка з метою архівування згідно з суспільними інтересами, а також для цілей наукового чи історичного дослідження або статистики не повинна вважатися несумісною з початковими цілями;
- *“мінімізація даних”* – передбачає обмеження тими персональними даними, які відповідають і необхідні для досягнення цілі, для яких вони обробляються. Не можна збирати персональні дані в більшому обсязі, ніж це було визначено для цілей обробки;
- *“точність”* – передбачає наявність адекватності персональних даних відомостям про суб’єкта даних, які мають постійно підтримуватися в актуальному стані. Неточні та застарілі персональні дані, з урахуванням цілі, для якої вони обробляються, слід видаляти або виправляти без затримки;
- *“обмеження зберігання”* – персональні дані повинні зберігатися у формі, що дозволяє ідентифікувати суб’єкта даних не довше, ніж це необхідно для цілі, для якої вони обробляються. Персональні дані можуть зберігатися протягом тривалішого періоду виключно для цілей архівації, інтересів наукових, дослідницьких, історичних і статистичних цілей. Регламент також уточнює, що компанії мають проводити регулярні перевірки з метою чищення носіїв даних (інформації);
- *“цілісність і конфіденційність”* – персональні дані повинні оброблятися у спосіб, що забезпечує належний захист, включаючи захист від несанкціонованої та незаконної обробки, випадкової втрати, знищення або пошкодження, з використанням відповідних технічних або організаційних заходів. Це функції контролерів, які повинні бути впевненими, що створені усі умови захисту та безпеки даних;
- *“підзвітність ”* – передбачає діяльність з: призначення у організаціях посадових осіб, що відповідають за захист персональних даних, ведення обліку, записів і перевірки дій з виконання принципів та порядку Регламенту.

Дія Регламенту не поширюється на обробку персональних даних, що стосується:

- обробки персональних даних фізичною особою у ході винятково особистої чи побутової діяльності та не пов’язаної з професійною чи комерційною діяльністю. Проте, Регламент застосовується до контролерів чи осіб, що здійснюють обробку даних, які забезпечують засоби для обробки персональних даних у ході такої особистої чи побутової діяльності;

- юридичних осіб, а також окремих підприємств. Проте, дія Регламенту поширюється на обробку персональних даних контролером або обробником, що пов’язана з пропозицією товарів або послуг та її контроль, які повинні здійснюватися незалежно від того, чи сама обробка відбувається у межах або поза межами Союзу. Моніторинг поведінки суб’єктів обробки даних тією мірою, якою їх дії відбуваються в межах Союзу, передбачає встановлення, чи відбуваються їх дії у мережі Інтернет, у тому числі потенційне використання технологій обробки персональних даних, що складається з профілювання фізичної особи, зокрема з метою прийняття рішень щодо неї чи нього або аналізу та передбачення її/його особистих уподобань, поведінки та настроїв;

- обробки персональних даних компетентними органами влади з метою запобігання, розслідування, виявлення чи судового переслідування кримінальних правопорушень, або виконання кримінальних покарань, у тому числі охорони і запобігання загрозам суспільній безпеці та вільне переміщення таких даних, що є предметом Директиви (ЄС) 2016/680 Європейського Парламенту та Ради [11, с. 107-158];

- файлів або груп файлів, а також їх титульних сторінок, не структурованих за конкретним критерієм;

- сфери національної безпеки та по відношенню до спільної зовнішньої політики та політики безпеки Союзу;

- анонімних відомостей про осіб, що померли;

- до діяльності судів та інших судових органів. Регламентом передбачена можливість доручити функції нагляду за такими операціями з обробки даних окремим органам судових систем держав-членів ЄС.

Розширення понять та визначень.

У Регламенті розширено поняття “персональні дані”, введені поняття “контролер”, “обробник” (“оператор” – *від авт.*), “відповідальний за захист персональних даних”, “профілювання”, “псевдонімізація”, “основна установа”, “наглядовий орган”, “заінтересований наглядовий орган”, встановлено “право на видалення” (“право бути забутим”), “право на переносимість даних”.

Згідно Регламенту “персональні дані” – це будь-яка інформація, яка стосується фізичної особи, що ідентифікована або може бути ідентифікована (“суб’єкт даних”); фізична особа, що може бути ідентифікована – це особа, яка може бути ідентифікована, прямо чи опосередковано, зокрема за такими ідентифікаторами, як ім’я, ідентифікаційний номер, відомості про місце розташування, он-лайн-ідентифікатор або на один чи декілька факторів, специфічних для фізичної, фізіологічної, генетичної, ментальної, економічної, культурної або соціальної ідентичності цієї фізичної особи.

Якщо раніше персональними даними вважалися тільки документи, що містять імена, адреси й т.ін., то зараз це визначення розширено. Дані, пов’язані з IP-адресами, е-поштою та cookie-файли[2], що зберігають суто індивідуальні відомості про користувача мережі також охоплюються положеннями Регламенту.

Існують певні типи персональних даних, що відносяться до категорії особливих або “чутливих” відомостей про особу. Це відомості, що розкривають расове або етнічне походження, політичні погляди, релігійні або філософські переконання і членство в профспілках. Крім того, згідно ст. 9 Регламенту, до цієї групи віднесені генетичні та біометричні дані, які можуть використовуватися для ідентифікації фізичної особи.

[2] Cookie – це файли, які автоматично копіюються з Інтернету на комп’ютер користувача і надають відомості про нього. Несанкціоновано отриману від cookie-файлу інформацію можна прив’язати до зібраних раніше файлів баз даних і одержати “портрет” користувача.

Важливим є те, що персональними вважаються тільки ті дані, за якими особу можна *ідентифікувати*. Наприклад, пошта містить ім’я, прізвище і е-адресу, тому відноситься до персональних даних, а окрема адреса е-пошти – ні; ім’я і номер телефону – персональні дані, телефон/адреса самі по собі – просто дані. Якщо з даних стає щось відомо про людину (її місце роботи, контакти і інше), то вони відносяться до персональних. Також, будь-які відомості, до яких було застосовано псевдонім, який може бути віднесено до фізичної особи за допомогою використання додаткової інформації, повинні розглядатися як відомості про фізичну особу, що може бути ідентифікована.

Права суб’єкта даних *(фізичної особи)***.**

Регламент значно розширює права громадян ЄС стосовно контролю за своїми персональними даними. Суб’єкти даних мають право запрошувати підтвердження факту обробки їх даних, місце і мету обробки, категорії оброблюваних персональних даних, яким третім особам вони розкриваються, період, протягом якого дані оброблятимуться, а також уточнюватимуть джерело їх отримання і вимагатимуть їх виправлення. Більш того, суб’єкт даних має право вимагати припинення обробки своїх даних.

Регламент встановлює високі вимоги до формі отримання згоді на обробку даних. Згода людини на обробку її персональних даних повинна бути визначена у формі однозначно чіткого твердження про відповідний дозвіл. Наприклад, повідомлення на сайті про те, що суб’єкт даних автоматично дав згоду на збір і обробку його персональних даних, не є згодою фізичної особи. Згода повинна бути надана в активній дії, наприклад, письмовою заявою, зокрема електронним способом.

Суб’єкт даних має право на виправлення персональних даних, що стосуються його або її. Комісія ЄС відстоює право кожного користувача Інтернету в ЄС мати також **“**право бути забутим**”**, тобто право на видалення його/її персональних даних та припинення обробки. Пошукові системи і соціальні мережі зобов’язані стирати фото-[3] і інші відомості про суб’єкта даних на його вимогу**.** Обробка фотографій не повинна розглядатися як обробка особливих категорій персональних даних**.**

Суб’єкт даних має право заперечувати проти обробки його даних, яка здійснюється з метою прямого маркетингу, у тому числі профілювання, до ступеню, в якому це пов’язано з таким маркетингом, стосовно як початкової, так і подальшої обробки.

Діти заслуговують на особливий захист їх персональних даних. Не можна вимагати згоду на обробку в контексті надання профілактичних або консультаційних послуг безпосередньо у дитини. Згода повинна бути авторизована батьками (або законними представниками дитини). Віковий поріг авторизації встановлюється державами-членами ЄС окремо (від 13 до 16 років).

Фізичні особи повинні бути обізнані про ризики, правила, гарантії та права стосовно обробки персональних даних та здійснення своїх прав стосовно такої обробки.

Кожен суб’єкт даних має право подати скаргу до національного наглядового органу, зокрема у державі-члені, де він чи вона постійно проживає, та право на ефективні засоби правового захисту. У випадку проваджень проти контролера або обробника позивач повинен мати можливість подавати позов до судів держав-членів, де розташовані установи контролера або обробника або де проживає суб’єкт даних, за винятком випадків, коли контролер є державним органом держави-члена, що діє при здійсненні своїх публічних повноважень.

[3] Згідно українського законодавства, зйомка в публічних місцях повністю дозволена, але на території ЄС слід пям’ятати про європейські правила.

Згідно Регламенту, немає конкретних вимог до ступеню, порядку і способу захисту даних – кожен може вибирати правові засоби сам. Найпопулярніші способи анонімізувать їх – шифрування або псевдонімізація. Псевдонімізація – один з технічних та організаційних заходів забезпечення рівня безпеки, який відповідає наявним ризикам. Вона припускає структурну зміну даних таким чином, щоб персональні дані не могли бути віднесені до конкретного суб’єкта. Відділення імені від решти даних і заміна його іншим ідентифікатором також буде псевдонімізацією.

Обробка особливих категорій даних.

Персональні дані, які, за своїм змістом, є особливо чутливими (расове, етнічне і національне походження, політичні, релігійні, світоглядні вірування, членство у політпартіях, профспілках, стан здоров’я, біометричні, генетичні дані, статтева орієнтація, притягнення до адміністративної або кримінальної відповідальності) заслуговують на особливий захист. Однак, обробка може бути необхідною для забезпечення суспільних інтересів у сферах охорони здоров’я, правоохоронної діяльності тощо без згоди суб’єкта даних.

Відхилення від заборони на обробку особливих категорій дозволяється у випадках, коли це передбачено законодавством Союзу або держави-члена та забезпечено відповідними гарантіями, з метою захисту персональних даних та інших прав, якщо це відповідає суспільним інтересам, зокрема – обробка персональних даних в сфері трудового права, законодавства про соціальний захист, у тому числі пенсії та охорона здоров’я, а також моніторинг, сповіщення, запобігання та контроль розповсюдження інфекційних захворювань та інших серйозних загроз здоров’ю. Такі відхилення можуть дозволятися з метою управління послугами в галузі охорони здоров’я, для забезпечення якості та економічної ефективності процедур, що використовуються для розгляду заяв щодо пільг та послуг у системі страхової медицини, або для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики. Крім того, відхилення повинно дозволяти обробку таких персональних даних, якщо це необхідно для створення, оформлення або захисту юридичних претензій, як в судовому процесі, так і в ході адміністративної або позасудової процедури.

Якщо в ході електоральної діяльності робота демократичної системи держави-члена потребує від політичних партій компіляції персональних даних щодо політичних переконань населення, обробка таких даних може бути дозволена з міркувань суспільних інтересів, за умови встановлення гарантій індивідуальної конфіденційності.

Обов’язки суб’єктів обробки *(компаній, підприємств, організацій тощо).*

Регламент має екстериторіальну дію для всіх держав-членів ЄС. Суб’єкт обробки буде мати справу тільки з одним національним органом із захисту даних, що знаходиться в країні ЄС, де розташовані їх основні установи.

Встановлено, що будь-які компанії не мають права пропонувати товари або послуги та передавати, у зв’язку з цим, персональні дані до країн ЄС, якщо рівень захисту у них нижчий, ніж в ЄС або якщо вони не дотримуються правил ЄС щодо захисту даних. Передача даних із країн ЄС у треті країни та міжнародні організації передбачено здійснювати тільки у повній відповідності до цього Регламенту.

Виходячи з вищевказаного, діяльність філіалів, представництв українських організацій на території ЄС повинна повністю відповідати його вимогам. Важливим є те, що організації, що обробляють персональні дані європейців в Україні, при здійсненні моніторингу суб’єктів даних, профілюванні окремих осіб, наприклад, для з’ясування їх поведінки і потреб, а також реалізації он-лайн-продажу (наприклад, ж/д-, авіа-, автобусне перевезення, готелі, хостели і ін.), також підпадають під дію Регламенту.

Регламентом визначена заборона на збір персональних даних будь-якою компанією (і державою) без дозволу з боку фізичних осіб – відповідних суб’єктів права на них. Винятки допускаються лише в тому випадку, якщо в країні існують законодавчі положення, які примушують до передачі даних, що містять відповідну інформацію.

Компанії зобов’язані видалити зі всіх своїх баз даних анкаунти і інші дані суб’єкта права на персональні дані за першою його вимогою. Це означає, що таки компанії, як Facebook, Google, Twitter, а також будь-які Інтернет-магазини (он-лайн-магазини), туроператори, транспортні та маркетингові компанії, які знаходяться, зокрема в Україні, та обробляють дані резидентів ЄС мають виконувати правило “право бути забутим” відповідних суб’єктів права на персональні дані. Це право не абсолютне – якщо обробка здійснюється за приписом закону, суб’єкт не може реалізувати це правило. Особливо це стосується правоохоронної та судової діяльності, про що йдеться у іншому документі “Пакету” – у Директиві ЄС 2016/680 [11, с. 107-158].

Суб’єкти обробки даних зобов’язані надавати безкоштовно електронну копію персональних даних іншої компанії на прохання самого суб’єкта персональних даних. Це “право на переносимість даних” також є новацією, що введена Регламентом.

Суб’єкти обробки даних зобов’язані повідомляти наглядові органи (а в деяких випадках і суб’єктів даних) про будь-які порушення, пов’язані з персональними даними, впродовж 72 годин після виявлення такого порушення.

Суб’єкти обробки даних повинні розробити та прийняти внутрішню політику компанії[3] з захисту та обробки персональних даних, включаючи розробку і впровадження Кодексу поведінки у сфері захисту даних (див. [12, с. 27-30]), які відповідають вимогам Регламенту, а також упровадити заходи, що відповідають принципам захисту (зокрема, мінімізація і псевдонімізація обробки персональних даних, надання суб’єктам даних можливості контролювати їх обробку), навчати персонал, проводити перевірки діяльності з обробки даних, вести документацію з процесів обробки, упроваджувати заходи по вбудованій системі захисту даних “за умовчанням” для забезпечення умов конфіденційності інформації.

Загальна організація забезпечення обробки та захисту персональних даних.

Згідно Регламенту, в практичній діяльності організацій щодо захисту персональних даних головними є суб’єкт даних, контролер та процесор (оператор).

Суб’єкт даних – це фізична особа, персональні дані якої обробляються.

Контролер (фізична чи юридична особа, державний орган, агенція або інша установа – т.з. “власник” бази даних), визначає мету і засоби отримання персональних даних і несе велику юридичну відповідальність, ніж процесор. По суті контролери визначають необхідні дії з персональними даними і відповідають за їх обробку**.** Контролер зобов’язаний вести реєстр всіх дій, які здійснюються в процесі обробки персональних даних. Також контролер повинен вжити належні технічні і організаційні заходи для забезпечення того, щоб за умовчанням оброблялися тільки персональні дані, необхідні для кожної конкретної мети обробки.

Процесор (фізична чи юридична особа, державний орган, агенція або інша установа – т.з. “оператори”) є виконавцем обробки (тобто той, хто працює з базою), за дорученням контролера.

Контролер і обробник можуть бути однією особою.

---

[3] У Додатку до цієї роботи надаються рекомендації щодо плану внутрішньої політики забезпечення захисту персональних даних у комерційних організаціях: за матеріалами посібника для бізнесу Федеральної торгової комісії США, які, як вважаємо, будуть корисними будь-кому.

Призначення відповідального за захист персональних даних. Ця вимога обов’язкова для: всіх державних органів; організацій, чиї види діяльності передбачають масштабний і систематичний моніторинг окремих осіб; організацій, чиї види діяльності передбачають обробку спеціальних категорій даних або даних, що відносяться до медичних записів, правопорушень і кримінально-звинувачувальних вироків (судимостей).

Будь-яка організація може призначити співробітника з захисту даних для управління процесами обробки і контролю за дотриманням вимог Регламенту. При цьому організація повинна опублікувати відомості про такого співробітника, а також направити її національному наглядовому органу з захисту персональних даних.

Посадова особа, що відповідає за захист даних, може бути співробітником контролера або процесора, або виконувати завдання на основі контракту про послуги.

Суб’єкти персональних даних можуть звертатись до посадової особи, що відповідає за захист даних, з усіх питань, пов’язаних з обробкою їх персональних даних та з реалізацією їх прав згідно з Регламентом.

Національні служби з захисту персональних даних.

Регламент спрямовано на посилення національних служб із захисту даних за умов повної їх незалежності, що є важливим компонентом захисту фізичних осіб у зв’язку з обробкою їх персональних даних. Згідно ст. 51, 53, 57 Регламенту, кожна держава-член законодавчо забезпечує та покладає на один або декілька незалежних публічних органів (“наглядові органи”) відповідальність за виконання завдань, встановлених цим Регламентом, для того, щоб захистити фундаментальні права та свободи фізичних осіб у сфері обробки та сприяти вільному руху персональних даних у межах Союзу. Компетенція наглядових органів не поширюється на контроль операцій з обробки в судах, що діють у якості судового органу (ст. 55 Регламенту).

Якщо у державі-члені створено декілька наглядових органів, необхідно на законодавчому рівні створити механізм узгодженості, для забезпечення ефективної їх діяльності. При цьому, держава-член зобов’язана визначити наглядовий орган, що діятиме як головна контактна особа.

Повноваження наглядових органів повинні включати в себе можливість накладати тимчасові або остаточні обмеження, у тому числі заборони, на обробку персональних даних. Повноваження для розслідування в частині доступу до приміщень повинні бути реалізовані відповідно до конкретних вимог процедурного права держави-члена, таких як вимога отримання попереднього судового дозволу.

Кожен наглядовий орган діє абсолютно незалежно під час виконання своїх завдань та здійснення повноважень згідно з Регламентом. Кожна держава-член повинна забезпечити наглядовий орган кадровими, технічними та фінансовими ресурсами, приміщеннями та інфраструктурою, необхідними для ефективного виконання їх завдань та реалізації повноважень. Кожен наглядовий орган повинен мати окремий публічний щорічний бюджет, який може бути частиною загального державного бюджету.

Що стосується повноважень наглядових органів отримувати від контролера або обробника доступ до персональних даних та до їх приміщень, держави-члени мають приймати підзаконні акти, в межах цього Регламенту, що встановлюють правила з метою гарантування професійних зобов’язань збереження таємниці, тією мірою, якою це необхідно для узгодження права на захист персональних даних, із зобов’язанням збереження професійної таємниці. Це не повинно обмежувати існуючі зобов’язання держав-членів щодо прийняття правил збереження професійної таємниці, як цього вимагає законодавство Союзу.

За порушення Регламенту, кожен наглядовий орган повинен мати повноваження для накладання адміністративних штрафів. Крім того, держави-члени мають можливість встановлювати правила щодо кримінальних покарань, за порушення національних правил, прийнятих в рамках Регламенту, а також в позбавленні вигоди, отриманої через порушення його приписів.

Санкції. Регламентом посилюється відповідальність за порушення його правил як до компаній в ЄС, так і до зарубіжних фірм, якщо вони обробляють персональні дані фізичних осіб, що знаходяться в ЄС – розмір штрафу встановлено до 20 мільйонів Євро або 4 % від загального річного обігу компанії за попередній фінансовий рік, залежно від того, яка сума більше.

Загально-соціальне упорядкування відносин.

Регламент визначає необхідність узгодження правил, що врегульовують свободу слова та інформації, у тому числі включаючи публіцистичну, академічну, художню та/або літературознавчу форму, з правом на захист персональних даних. Обробка та зберігання персональних даних виключно для цілей журналістики або для академічного, художнього чи літературного виразу повинна підлягати звільненням від деяких положень цього Регламенту, якщо це необхідно для узгодження права на захист персональних даних та “права на свободу висловлювати свою думку і свободи інформації”, закріплених Статтею 11 Хартії (Статуту – *від авт.*) основоположних прав Європейського Союзу [13]. Це також стосується і обробки персональних даних у аудіо- та візуальній формі, у архівах новин та прес-бібліотеках. Винятки та відхилення повинні прийматися враховуючи права суб’єкта даних, контролера та обробника, передачу персональних даних до третіх країн або міжнародних організацій, незалежність наглядових органів та узгодженість в їх співпраці. Якщо такі винятки та відхилення відрізняються у різних державах-членах, повинен застосовуватися закон тієї держави-члена, яким керується контролер. Для врахування важливості права на свободу слова у будь-якому демократичному суспільстві, необхідна широка інтерпретація понять, що стосуються такої свободи, наприклад, у журналістиці.

Зберігання персональних даних має також бути законним, якщо це необхідно, для виконання юридичних зобов’язань або при виконанні службових повноважень, наданих контролеру, на підставі суспільного інтересу в галузі охорони здоров’я, або для архівних цілей, для цілей наукового чи історичного дослідження або статистики, або для створення, оформлення або захисту юридичних претензій.

Обробка персональних даних для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики має бути забезпечена відповідними гарантіями для прав і свобод суб’єкта даних згідно з цим Регламентом. Ці гарантії повинні мати технічні та організаційні заходи з метою забезпечення, зокрема, принципу мінімізації даних. Зазначена обробка персональних даних також повинна виконуватись за умови проведення контролером оцінки доцільності досягнення таких цілей через обробку даних, що не допускають ідентифікації суб’єктів даних, за умови існування відповідних гарантій (таких як, наприклад, псевдонімізація даних). Держави-члени повинні мати повноваження вводити, за особливих умов та за наявності відповідних гарантій для суб’єктів даних, специфікації та відхилення стосовно інформаційних вимог та прав на виправлення, видалення, права бути забутим, на обмеження обробки, на переносимість даних та права на заперечення при обробці персональних даних для архівних цілей відповідно до суспільних інтересів, для цілей наукового чи історичного дослідження або статистики. Умови та гарантії, про які йде мова, можуть вимагати особливих процедур для суб’єктів даних з метою реалізації таких прав, якщо це доцільно з урахуванням цілей

особливої обробки разом з технічними та організаційними заходами, спрямованими на мінімізацію обробки персональних даних на виконання принципів пропорційності та необхідності. Обробка персональних даних для наукових цілей також повинна відповідати іншим діючим законодавчим актам, таким як закони щодо клінічних випробувань. При цьому необхідно, зокрема, встановити особливі умови стосовно публікації або іншого способу розкриття персональних даних. Статистичні цілі передбачають, що результати обробки для цілей статистики не є персональними даними, але є узагальненими даними, і що її результат не використовується для рішень стосовно конкретної фізичної особи.

Згідно Регламенту доступ громадськості до офіційних документів може вважатися таким, що відповідає суспільним інтересам.

Підходи до захисту персональних даних в США.

Впродовж багатьох років Сполучені Штати і Європа по-різному підходять до захисту персональних даних. Деякі посадовці Сполучених Штатів стверджують, що не дивлячись на різні підходи, результати рівні. *“Сума форм захисту приватного життя в США рівна або більше, ніж одна форма у всьому Європейському Союзі”*, вважає Камерон Ф. Керрі [14], головний радник Міністерства торгівлі, що керує Агентством, зусилля якого спрямовані на допомогу різним галузевим групам, розробникам додатків, чия робота дуже слабо регулюється і особливо часто призводить до несанкціонованого збору і використання відомостей про споживачів, що є основною причиною гострих дискусій між американською корпорацією Google та представниками Комісії ЄС. Більш того, американські урядовці, торгові групи і технічні керівники, закликали законодавців Брюсселя переглянути реформу, яка здійснюється, оскільки, як вони вважають, єдине регулювання і універсальний підхід не можуть бути ефективними. Американські представники галузі телекомунікацій відзначають, що немає нічого більш прийнятного для торгівлі, ніж вільний Інтернет. “*Це не мудро мати одне надмірно широке регулювання, що закріплює підхід – “один розмір для всіх”, який перешкоджатиме або підриватиме здібність компаній до інновацій в глобальній економіці”,* говорить Кевін Річардс, старший віце-президент Федерального уряду, що відповідає за TechAmerica – торгову групу, яка представляє інтереси таких компаній, як Google і Microsoft. Для посадовців Сполучених Штатів і торгових груп деякі положення реформи здаються дуже жорсткими. Вони стверджують, що американський підхід, де застосовуються галузеві закони про конфіденційність на додатки до саморегулювання і контролю з боку органів Федеральної торгової комісії – є вдаліший.

У 2012 р. Президент США Барак Обама запропонував “Біль про право споживачів на конфіденційність” (Consumer Privacy Bill of Rights), який надав американцям багато з тих же базових прав і форм захисту, що і правила, які містяться в Регламенті ЄС. Вони включають: право на доступ до записів персональних даних в компаніях, право на виправлення цих записів і право обмеження персональних даних, які компанії збирають і зберігають. Але у 2017 р. Палата представників Конгресу і, далі, Сенат США проголосували резолюцію про скасування цього закону, що зобов’язує, зокрема, Інтернет-провайдерів одержувати дозвіл на використання персональних даних (запитувати) користувачів, включаючи, таке, як місцеположення клієнта і історія його перегляду Інтернет-сайтів. Прихильники скасування закону (Verizon, AT&T, Comcast і ін. представники крупних корпорацій ринку комунікацій) стверджують, що це підвищить конкуренцію на ринку. Але критики зазначають, що скасування закону сильно ударить по правам суб’єктів даних. Ричард Блументал, член Демократичної партії і сенатор США від Коннектикуту, назвав цю резолюцію *“прямою атакою на права людей, на приватність і на*

правила, які забезпечують, сприйманий як належне, базовий захист від нав’язливого і незаконного втручання корпорацій у використання соцмереж і веб-сайтів” [15].

Виходячи з того, що закон 2012 р. з великою вірогідністю буде остаточно скасований і Палатою представників, і Президентом Трампом, необхідна розробка нового набору правил забезпечення конфіденційності для Інтернет-провайдерів. Вони, можливо, будуть схожі на старі, накладаючи обмеження на використання відомості про дітей та про здоров’я, але в них не буде обмежень використання історії проглядання веб-сторінок, несанкціонованого застосування для комерції та ін. Тобто, Інтернет-провайдери одержать саме те, що хочуть, тоді як персональні дані суб’єктів даних знову будуть збиратися та продаватися.

Про поширення у світі активної комерціалізації персональних даних вже не раз повідомлялося, і Україна не виняток [16; 17]. Процес збору, обробки і поширення персональних даних давно перетворився на процвітаючий бізнес, а ринок персональних даних ще у 2006 р. досягав не менш як 3 млрд. доларів у рік [18]).

Крупні в США компанії по збору персональних даних, наприклад, Metromail, First Data Solution, Acxiom, володіють даними не менш як про 90 млн. сімей і 140 млн. людей. У їх базах зберігається, обробляється, а потім продаються відомості про ім’я, дні народження, адреси, паспортні дані, номера телефонів та телефонні дзвінки, родичів, свідоцтва, довідки, зміст різних квитанцій, розмір доходів і податків, об’єкти та предмети власності, подорожи, хвороби людини і ліки, які вона приймає та багато ін.

Легальні фірми з продажу інформації в США, як правило, засновані приватними детективами, що були поліцейськими або співробітниками служб безпеки. Те, що вони продають, часто не вважається секретною інформацією. Більш того, жоден федеральний закон США не захищає конфіденційність відомостей щодо історій хвороби, банківських рахунків, телефонних номерів і рахунків за телефонні послуги тощо. А суб’єкти підпільної мережі збирають і продають персональні дані, навіть якщо вони одержані незаконним шляхом. Складність боротьби з такою діяльністю полягає у тому, що багато фірм, що займаються інформаційним бізнесом, приходить і йде, міняє назви, закриває свої вузли в Інтернет і відкриває нові. Поки та якщо який-небудь представник влади захоче придивитися до такої діяльності, підпільний торговець міняє свою адресу та зникає.

Стан справ в Україні.

В Україні основним законом, що регулює відповідні відносини, є Закон України “Про захист персональних даних” від 2010 р. Проаналізувавши положення його різних редакцій (див. [9]), можна вважати українське законодавство прогресивним в контексті напрямів приписів Регламенту (зокрема включаючи принципи обробки, порядок отримання згоди суб’єкта, перелік категорій персональних даних із спеціальним статусом, прав суб’єктів і обов’язків володільців/розпорядників та ін.).

Проте, законодавство України поки не повністю відповідає деякім приписам Регламенту, зокрема, які передбачають обов’язкову наявність у державі системно-незалежної організаційної структури забезпечення захисту персональних даних, здатної ефективно працювати в умовах застосування інформаційно-комунікаційних технологій і великомасштабних мережевих систем передачі даних.

Відсутність ефективної загальнодержавної організаційної системи і дієвих механізмів захисту персональних даних, за умов обов’язкової відповідальності за правопорушення інформаційних відносин, ускладнюється низькою правовою поінформованістю громадян про можливості боротьби з несанкціонованим використанням та продажем їх персональних даних у різних, не виключено, шахрайських та маніпулятивних інтересах. В умовах слабкої організаційної активності держави в практичній боротьбі з порушеннями законодавства, люди, з різних обставин, зокрема, судово-процесуальними складнощами, не дуже

бажають займатися захистом та безпекою своїх персональних даних, хоча вони можуть складати предмет не тільки адміністративного, але й кримінального злочину. Як зазначається у [19]: *“…по діючому у нас закону “Про захист персональних даних” штрафні санкції за порушення складають максимум 200 неоподатковуваних мінімумів доходів громадян, а це 3,4 тис. грн. При цьому, керівнику фірми, що розповсюдив персональні дані громадян без їх згоди, можуть на перший раз просто виписати розпорядження – як би покартати. Якщо порушення повториться, то справа може дійти і до штрафу. А постраждалий через розповсюдження його персональних даних може звернутися до суду, зажадавши від кривдника виплатити йому моральний збиток. Якщо він доведе, як сильно постраждав через поширену інформацію, то може навіть одержати компенсацію морального збитку. Але це для нас – тільки теорія”.*

Головне тут у тому, що різні уявлення різних суб’єктів про тлумачення понять та категорій продовжує залишатися і, мабуть, завжди буде проблемою.

Суб’єкт даних (наприклад, постраждалий) може трактувати захист своїх персональних даних, як сам хоче. Питання у тому – а чи будуть компетентні органи тлумачити так само, і чи зуміє він в суді відстояти саме своє тлумачення?

Сьогодні чинними є понад 100 міжнародно-правових актів (Конвенцій, Протоколів, Директив, Рекомендацій ООН, РЄ, ЄС, ОБСЕ тощо), які прямо або опосередковано відносяться до правового регулювання захисту персональних даних (деякі з них див. у посібнику [1]). Вони мають дуже значну кількість декларацій та приписів, які не завжди сприймаються однозначно й зрозуміло, створюють можливість різних суб’єктивних тлумачень. При цьому вважається, що “заклики” та приписи повинні спрямовуватися на охоплення усіх випадків використання персональних даних людини у різноманітності життя. Але у всіх них ***відсутнє головне – вони не визначають універсально-загального критерію, як визначального фактора та мирила оцінки різних суб’єктивних уявлень***, на базі чого має оцінюватися та здійснюватися захист персональних даних людини в контексті її основоположних прав і свобод. Можливість запровадження вказаного критерію, в принципі, передбачена ще в 1981 році ст. 11 Конвенції РЄ № 108: *“Жодне з положень цієї глави не тлумачиться як таке, що обмежує або іншим чином перешкоджає можливості Сторони забезпечувати суб’єктам даних більший ступінь захисту, ніж передбачено цією Конвенцією”.*

На початку розробки проекту Закону України “Про захист персональних даних”, пропонувалось та аргументувалось (ще у 1998 р. та далі у інших роботах, зокрема у [20 – 23]) можливість запровадження у законодавство України такого, як ми вважали, *універсального критерію – “право власності людини на свої персональні дані”*, за умов обов’язкового забезпечення інтересів національної безпеки, економічного добробуту та прав людини. Іншими словами, пропонувалось основу захисту персональних даних розглядати, як *предмет особливо-унікального виду*, який юридично має *умовну форму права власності*, монополія на яке обмежується виключно законом.

Пізніше було запропоновано дещо інше визначення вищезазначеної категорії – *“право приватної власності людини на свої персональні дані”*, про що йдеться у [24].

Відповідь була та є незмінною – “персональні дані відносяться до особистих немайнових прав”. Й це стверджується у часи, коли завдяки сучасним інформаційним технологіям персональні дані людини активно та не санкціоновано збирають, пропонують у мережах та продають. Для будь-якої діяльності, зокрема пов’язаною з комерцією, персональні дані давно стали предметом та товаром, які не тільки збільшують матеріальні цінності і практично використовуються як звичайний об’єкт продажу/покупки, але вже є складовою світового ринку.

Проте, у законодавстві України до них продовжують застосовувати поняття “немайнові права”[4], з пристосуванням до нього слова “особистих”.

Початок цього було покладено в ЦКУ, а потім потрапило і в різні закони, зокрема, щодо персональних даних. Загальне словосполучення сприймається як тавтологія – “масло масляне” (у логіці – це помилка “порочного кола”) та сприяє підтримці “системи захисту”, яка в умовах застосування електронно-інформаційних засобів може функціонувати на підставі суб’єктивних уявлень вибіркової модальності про предмет судження.

Таким чином, з одного боку, маємо не вирішену юридичну суперечність між економічними реаліями використання персональних даних і їх статусом в законодавстві, а з іншого – поширену публічну риторику необхідності боротьби за свободи і права, хоча, нерідко, це має характер боротьби проти свободи і прав інших. І це все при тому, що захист цінової вартості відомостей, які складають інформаційний продукт під назвою “персональні дані”, не тільки забезпечує соціальний захист прав і свобод людини, але і складає економічний аспект у безпеці людини, які завжди пов’язані між собою.

До вказаного можна додати, у 2015 році було повідомлення [25] про те, що в Раді Європи почала здійснюватися робота по модернізації Конвенції Ради Європи № 108 та розробці *“універсальних норм розвитку соціальної взаємодії”*.

Висновки.

1. У травні місяці 2018 року вступили у дію нові екстериторіального принципу дії правила і порядок захисту персональних даних (“Пакет захисту даних”) для держав-членів ЄС, а також рекомендації до їх впровадження іншими країнами, що співпрацюють з ЄС, які так чи інакше обробляють дані осіб, що знаходяться в ЄС. Головним документом “Пакету” є Регламент ЄС 2016/679 від 27 квітня 2016 року.

Нові вимоги до обробки та захисту персональних даних досить серйозні та складні. Але в них є важлива позитивна сторона: легше дотримуватися єдиного набору правил захисту, обробки та поширення даних, ніж враховувати національні нюанси щодо персональних даних кожної окремої країни ЄС, як це доводилося робити до введення Пакету. Дотримання одного правила замість 28 (країн-членів ЄС) створює умови допомоги малим підприємствам і фірмам, що розвиваються, вийти на нові ринки. Комісія ЄС запевняє, що реформа спрямована на стимулювання економічного зростання шляхом скорочення витрат і бюрократії для компаній, що працюють в ЄС.

Для усіх держав-членів ЄС визначається необхідність підняття рівня організаційно-правової діяльності та суттєвого удосконалення національних механізмів захисту персональних даних в умовах розвитку та поширення інформаційно-комп’ютерних технологій. Це, перш за все, стосується необхідності підвищення ефективності у діяльності національних уповноважених (наглядово-регулюючих) органів.

2. Україна в питаннях захисту персональних даних спирається на європейські правові стандарти та міжнародно-правовий досвід. Але загальна організація захисту персональних даних в Україні потребує реформування. У держави немає достатньої законодавчої бази і єдиної структурно-регулятивної системи захисту персональних даних, що не сприяє поліпшенню та ефективності роботи в сучасних технологічних умовах. Держава, на жаль, не дуже проявляє активність у боротьбі з правопорушеннями у цій сфері.

Новий порядок захисту та забезпечення безпеки персональних даних, що визначається Регламентом (ЄС) 2016/679, встановив одну з головних умов – рівень та організація захисту прав фізичних осіб стосовно обробки їх персональних даних повинні

[4] До речі, ні в одному з міжнародно-правових актів або національних законів застосування до персональних даних такого словосполучення як *“особисті немайнові права”* взагалі не існує.

бути еквівалентними не тільки в усіх державах-членах ЄС, але і у інших країнах, яки мають з ними будь-які стосунки. Інакше відмінності у захисті прав фізичних осіб, зокрема того, що стосується обробки, використання та поширення персональних даних, можуть стати на заваді вільному обігу персональних даних та бути перешкодою для здійснення економічної діяльності з державами-членами Союзу. Ці обставини вимагають більш узгодженої структури загальнодержавної організації захисту персональних даних, за умов жорсткого контролю дотримання правил європейських правових стандартів, що може сприяти розвитку цифрової економіки у межах внутрішнього ринку та співпраці з державами ЄС.

Головне – фізичні особи в Україні повинні мати законодавчу можливість контролю застосування своїх персональних даних та гарантій про надання на це особисто-визначеної ними інформованої згоди. Цьому може сприяти запровадження в українське законодавство універсально-загального критерію – *“право приватної власності людини на свої персональні дані”*, монополія на яку обмежується виключно законом в інтересах національної безпеки, економічного добробуту та прав людини.

На превеликий жаль, задача примусити більше хвилюватися про це законодавця продовжує залишатися актуальною.

Додаток

Забезпечення захисту персональних даних у комерційних організаціях:

за матеріалами посібника для бізнесу Федеральної торгової комісії США [26].

План захисту персональних даних базується на 5 основних принципах:

1. ***Здійснення інвентаризації.*** Необхідно знати, які персональні дані та особисті відомості зберігаються у ваших архівах та на комп’ютерах.
2. ***Зменшення обсягів особистих відомостей та даних, що зберігаються.*** Необхідно зберігати тільки те, що потрібно для здійснення вашого бізнесу.
3. ***Захист відомостей та даних.*** Необхідно забезпечити захист особистих відомостей та відповідних даних у захищеному від стороннього доступу місці.
4. ***Видалення даних***. Необхідно ретельно ліквідувати те, що вам більше не потрібно.
5. ***Планування.*** Необхідно мати план реагування на випадки порушення захисту та безпеки даних.

Стаття 1. Здійснення інвентаризації

Ефективний захист даних починається з оцінки того, яку інформацію ви маєте, і з визначення того, хто має доступ до неї. Розуміння того, як персональні дані потрапляють до компанії, як переміщуються всередині і як виходять з неї, а також, хто має або може мати доступ до них, є важливим для оцінки слабких місць в системі захисту даних. Тільки після дослідження, як персональні дані переміщуються, можливо визначити способи для їх захисту.

1. Інвентаризуйте всі комп’ютери, ноутбуки, флеш-диски, диски, домашні комп’ютери та інше обладнання для того, щоб визначити, чи зберігає ваша компанія дані, які визначають інформаційну конфіденційність. Також необхідно здійснити структурування даних, якими ви володієте, за типом та місцезнаходженням: файли з даними і комп’ютерні системи є основними носіями даних або ваша компанія отримує персональні дані багатьма способами – через веб-сайти, від підрядників, через кол-центри і тому подібне. Щодо даних, які зберігаються на ноутбуках, домашніх комп’ютерах персоналу та флеш-дисках, інвентаризація буде вважатися закінченою тільки після того, як буде перевірено всі дані, які мають конфіденційність.

2. Відслідковуйте персональні дані у вашій компанії шляхом розмов з відділами продаж, персоналом з відділу інформаційних технологій, відділом кадрів, бухгалтерією і іншими відділами, що надають послуги. Отримайте повну картину щодо того:

(a) ***Хто відправляє персональні дані у вашу компанію*** – чи отримуєте ви її від клієнтів?; компаній, що займаються кредитними картками?; банків чи інших фінансових інститутів?; кредитних бюро?; інших компаній?

(b) ***Як ваша компанія отримує персональні дані*** – вони потрапляють через: веб-сайти?; електронну пошту?; пошту?, передаються через касові апарати в магазинах?

(c) ***Який вид інформації ви отримуєте на кожній вхідній точці*** – чи отримуєте ви інформацію щодо кредитних карток через Інтернет?; чи зберігає ваш бухгалтерський відділ інформацію про рахунки клієнтів до запитання?

(d) ***Де ви зберігаєте інформацію, що отримуєте на кожній вхідній точці*** – чи це централізована електронна база даних на індивідуальних ноутбуках, на дисках чи дискетах, в папках, філіях?; Чи знаходяться будь-які файли з даними вдома у ваших працівників?

(e) ***Хто має або може мати доступ до персональних даних*** – хто з працівників має дозвіл на доступ до даних?; чи може хтось ще отримати його? – зокрема щодо компаній, які встановлюють та оновлюють програмне забезпечення, яке ви використовуєте для обробки даних з кредитними картками?

3. Різні види даних – різні ризики. Звертайте особливу увагу на те, як ви зберігаєте дані, що ідентифікують особу: номери соціального захисту, інформацію щодо кредитних карт, фінансову інформацію та персональні дані. Це те, що злодії використовують найчастіше для того, щоб здійснити шахрайство чи крадіжку.

Стаття 2. Зменшення обсягів інформації, що зберігається

Якщо для бізнесу не має необхідності в силу дії законодавства у зберіганні персональних даних, не зберігайте їх. А краще, не збирайте їх. Якщо ж для бізнесу необхідні певні персональні дані, зберігайте їх тільки до тих пір, допоки вони вам необхідні.

1. Використовуйте номери соціального захисту тільки для необхідних та законних цілей, наприклад, для звітів про податки із сум, що виплачуються працівникам.

2. Закон вимагає від вас скоротити чеки по кредитних та дебетних картках, які надаються в електронному вигляді вашим клієнтам. Ви можете включити не більше ніж п’ять останніх значень картки, і повинні видалити дату закінчення.

3. Не зберігайте дані щодо кредитних карток клієнтів, якщо ці дані не потрібні для вашого бізнесу. Наприклад, не зберігайте номер рахунку та дату закінчення, якщо не маєте суттєвої потреби для їх зберігання. Зберігання такої інформації довше ніж це необхідно – підвищує ризик того, що відомості можуть бути використані через крадіжку чи шахрайство.

4. Перевіряйте стандартні налаштування вашого програмного забезпечення, яке зчитує номери кредитних карток клієнтів і обробляє трансакції. Іноді воно налаштоване на постійне зберігання даних. Змініть стандартні налаштування, для того щоб впевнитись, що ви не зберігаєте дані, які вам не потрібні.

5. Якщо необхідно зберігати дані для вашого бізнесу або у силу дії законодавства, розробіть задокументовану політику такого зберігання для того, щоб визначити, які дані повинні зберігатися, як захистити їх, як довго їх зберігати і як розпорядитись ними, забезпечуючи безпеку таких даних, коли вони вам більше не потрібні.

Стаття 3. Зберігання інформації у захищеному від стороннього доступу місці

Який найкращий спосіб захисту персональних даних, які необхідно зберігати? Це залежить від виду даних та того, як вони зберігаються. Найбільш ефективні плани зберігання даних базуються на ключових елементах: фізична безпека, електронна безпека, навчання персоналу та практика щодо безпеки підрядників та постачальників послуг.

3.1. Фізична безпека

1. Зберігайте паперові документи чи файли, а також CD-диски, жорсткі диски, драйвери, касети і резервні копії, що містять персональні дані, в кімнатах, що закриваються на замок, та в закритих папках. Обмежте доступ працівників тільки доступом для законних цілей необхідних для бізнесу. Контролюйте, хто має ключі і їх кількість.

2. Вимагайте, щоб відомості, які містить персональні дані, зберігалися в закритих папках. Нагадуйте працівникам не залишати документи з конфіденційною інформацією на столах та відкриті файли з персональними даними, після того як вони залишають свої місця.

3. Вимагайте від працівників класти документи на місце, вимикати їх комп’ютери і закривати папки з файлами і офісні двері по закінченню робочого дня.

4. Впроваджуйте необхідний контроль за доступом до будівлі вашої компанії. Розказуйте працівникам, що робити і кому дзвонити, якщо вони бачать незнайому особу.

5. Якщо є склади, обмежте доступ працівників тільки доступом у законних цілях, необхідних для бізнесу. Відслідковуйте, хто і коли має доступ до даних, що зберігаються на складі.

6. Якщо ви пересилаєте конфіденційну інформацію, використовуючи зовнішніх кур’єрів чи підрядників, зашифруйте дані і сформуйте перелік даних, що пересилаються.

3.2. Електронна безпека

Безпека комп’ютера є не тільки справою персоналу відділу інформаційних технологій. Ви повинні знати уразливості вашої комп’ютерної системи і слідувати порадам експертів у цій сфері.

3.2.1. Загальна безпека інформаційної мережі

1. Визначте комп’ютери чи сервери, де зберігаються персональні дані.

2. Визначте всі можливості підключення до комп’ютерів, де зберігаються персональні дані. Це може бути Інтернет, електронні касові апарати, комп’ютери у ваших філіях, комп’ютери, що використовуються вашими постачальниками послуг з підтримкою вашої інформаційної мережі, і бездротові пристрої, наприклад, стільникові телефони.

3. Оцініть слабкі місця для загальновідомих та обґрунтовано передбачуваних нападів під час кожного підключення.

4. Не зберігайте персональні дані на будь-якому комп’ютері, що підключений до Інтернету, окрім випадку, якщо це необхідно для ведення бізнесу.

5. Зашифровуйте персональні дані, які ви надсилаєте іншим особам по загальній мережі (Інтернет), і відслідковуйте зашифровані дані, що зберігаються у вашій мережі або на дисках чи портативних пристроях зберігання даних. Відслідковуйте відправлення електронної пошти в рамках вашої бізнес-діяльності, якщо вони містять персональні дані.

6. Регулярно встановлюйте сучасні антивірусні програми на персональних комп’ютерах і серверах вашої мережі.

7. Регулярно перевіряйте спеціалізовані веб-сайти і сайти ваших продавців програмного забезпечення на предмет наявності нових версій і впроваджуйте політику встановлення оновлень, що затверджені продавцями.

8. Перевіряйте комп’ютери вашої мережі на предмет визначення робочих систем та послуг мережі. Якщо ви знайдете програми, які вам не потрібні, деактивуйте їх, щоб запобігти потенційним проблемам щодо безпеки. У разі якщо електронна пошта чи Інтернет не потрібен на конкретному комп’ютері, розгляньте можливість закриття портів для таких послуг на цьому комп’ютері для того, щоб запобігти неавторизованому доступу до цього комп’ютера.

9. Коли ви отримуєте дані щодо переказів по кредитних картках і інші фінансові дані, використовуйте Протокол захищених сокетів[5] або інші види безпечного зв’язку, які захищають дані під час відправки.

10. Звертайте особливу увагу на безпеку ваших Інтернет-додатків – програмного забезпечення, що використовується для того, щоб надати дані відвідувачам вашої веб-сторінки і для отримання даних від них. Інтернет-додатки можуть частково бути пошкоджені хакерськими нападами. Під назвою “напад шляхом ін’єкції” хакери встановлюють команди, які націлені на зловмисні дії, що виглядають як законний запит даних. При цьому хакери у вашій системі пересилають дані з вашої мережі на їх комп’ютери. Відносно легкий захист від таких нападів доступний з багатьох ресурсів.

[5] Протокол, що гарантує безпечну передачу даних через мережу, комбінуючи криптографічну систему з відкритим ключем і блочне шифрування даних.

3.2.2. Управління паролями

1. Контролюйте доступ до даних, що містять конфіденційну інформацію, шляхом встановлення вимоги до працівників використання “сильних” паролів. Експерти з технічної безпеки кажуть, що чим довший пароль, тим це краще. Так як легкі паролі, такі як часто вживані слова, можна легко вгадати, вимагайте, щоб працівники вибирали паролі, які міститимуть літери, числа і символи. Вимагайте, щоб логін та пароль були різними і часто змінювалися.

2. Пояснюйте працівникам, чому надання будь-кому свого паролю або його запис будь-де за межами робочого приміщення є дією проти компанії.

3. Використовуйте програму захисту екрану, яка автоматично виключає комп’ютер працівника після певного періоду його не активності.

4. Відключайте користувачів, які ввели неправильний пароль певну кількість разів.

5. Попереджайте працівників про можливі крадіжки персональних даних шляхом запиту паролів. Повідомляйте працівникам, що запит їх пароля являється незаконною дією і що ні в кого не повинні вимагати розкриття їх пароля.

6. При інсталяції нового програмного забезпечення одразу ж змініть стандартні паролі продавців або постачальників на більш безпечні і надійні паролі.

7. Застерігайте працівників відправляти персональні дані (зокрема, номери соціального захисту, паролі, дані щодо рахунків) електронною поштою. Незашифровані електронні листи не є безпечним способом відправки даних.

3.2.3. Безпека ноутбуків

1. Обмежуйте використання ноутбуків тільки тими працівниками, які потребують їх для виконання їх роботи.

2. Оцініть, чи потрібно персональні дані дійсно зберігати на ноутбуці. Якщо ні, видаліть їх спеціальною програмою з їх очистки. Видалити файли, використовуючи стандартні команди, недостатньо, тому що дані можуть залишитися на жорсткому диску ноутбуку. Програми з очистки даних можливо придбати в більшості спеціалізованих магазинів.

3. Вимагайте від працівників збереження ноутбуків у безпечних місцях.

4. Дозволяйте користувачам ноутбуків мати лише доступ до персональних даних, а не зберігати їх на ноутбуках. Дані мають зберігатися на головних комп’ютерах, ноутбуки повинні використовуватися тільки як пристрої, що відображають дані з головного комп’ютера, але не зберігають їх. Інформація може бути також захищена шляхом використання смарт-карт, засобів зчитування відбитків пальців та ін., а також паролів для доступу до головного комп’ютера.

5. Якщо ноутбук містить дані, шифруйте та кодуйте їх так, щоб користувачі не могли завантажити програмне забезпечення або змінити налаштування щодо захисту без погодження спеціалістів відділу програмного забезпечення компанії. Розгляньте можливість використання автоматично функції знищення для того, щоб дані на комп’ютері, які викрадено, були знищені, як тільки грабіжник намагатиметься використовувати їх в Інтернеті.

6. Навчайте працівників дотримуватися безпеки даних під час подорожі. Вони ніколи не повинні залишати ноутбуки в машинах на видноті, в місцях для багажу в готелях або здавати в багаж, якщо тільки це не вимагається безпекою аеропорту. Кожен, хто проходить через безпеку аеропорту, повинен слідкувати за своїм ноутбуком.

3.2.4. Захисна система

1. Використовуйте захисні системи для того, щоб захистити ваш комп’ютер від нападів хакерів, якщо він підключений до Інтернету. Захисні системи є програмним забезпеченням або обладнанням, яке розроблено для того щоб блокувати входження хакерів на ваш комп’ютер. Належним чином налаштована захисна система зробить важчим можливість хакерів знайти ваш комп’ютер та ввійти у ваші програми та файли.

2. Визначте, чи необхідно вам встановлення “обмеженої” захисної системи під час підключення до Інтернету. “Обмежена” захисна система відділяє вашу локальну мережу від Інтернету і може запобігти нападам шляхом спроб увійти в комп’ютер, де ви зберігаєте персональні дані. Встановіть “контроль за входом” – налаштування, що визначають, хто

пройшов через захисні системи і що вони бажають побачити – для того щоб дати можливість заходити до мережі тільки тим працівникам, до яких є довіра і їм необхідний такий доступ для законних потреб вашого бізнесу.

3. Якщо деякі комп’ютери вашої мережі зберігають персональні дані, а інші не зберігають, розгляньте можливість використання додаткових для них захисних систем або засобів.

3.2.5. Бездротовий та дистанційних доступ

1. Визначте, чи використовуєте ви бездротові пристрої, такі як сканери або стільникові телефони, що підключені до вашої комп’ютерної мережі або якими передаються персональні дані.

2. Якщо ви використовуєте бездротові пристрої, розгляньте можливість їх обмеженого підключення до вашої комп’ютерної мережі. Шляхом обмеження бездротових пристроїв, що можуть підключатися до вашої мережі, ви зробите доступ незнайомців до мережі важчим.

3. Для того щоб ускладнити для сторонніх осіб можливість читати документи, що містять конфіденційну інформацію, розгляньте можливість їх шифрування за допомогою електронних засобів.

4. Розгляньте також можливість використання шифрування, якщо вам необхідний дистанційний вхід до вашої комп’ютерної мережі, працівниками або постачальниками послуг, такими як компанії, що виявляють неполадки та оновлюють програмне забезпечення, що ви використовуєте для того, щоб обробляти покупки по кредитних картках.

3.2.6. Виявлення порушень

1. Якщо трапляються порушення в роботі мережі, розгляньте можливість використання систем, що визначають такі порушення. Для їх ефективності вони потребують частого оновлення для того, щоб бути націленими на нові типи хакерства.

2. Підтримуйте центральні реєстраційні файли даних конфіденційної інформації з метою перевірки діяльності в мережі для відслідковування та реагування на напади. Якщо на мережу здійснено напад, в такому файлі будуть міститися дані про комп’ютери, яким загрожують ризики.

3. Перевіряйте вхідний трафік, на який хтось з хакерів намагається скоїти напад. Слідкуйте за діяльністю нових користувачів, кількістю спроб невідомих користувачів або комп’ютерів увійти в систему, а також більш високим та більшим, ніж середній трафіком у незвичний для цього час доби.

4. Перевіряйте вихідний трафік з ціллю відслідковування порушень захисту персональних даних. Звертайте увагу на занадто великі розміри даних, що передаються з вашої системи до невідомих користувачів. Якщо велика кількість даних передається з вашої мережі, впевніться, що така передача здійснена на законних підставах.

5. У відповідь на порушення захисту даних вам необхідно мати і впроваджувати план дій.

3.3. Навчання персоналу

Ваш план захисту персональних даних може виглядати дуже гарним на папері, але він буде настільки сильним, наскільки сильний персонал, що впроваджує його. Виділіть час для того щоб пояснити правила вашому персоналу і навчити їх виявляти слабкі місця в безпеці даних. Періодичні тренінги підкреслюють важливість практичного застосування захисту даних. Добре навчена робоча сила являється найкращим захистом проти порушень захисту даних.

1. Перевіряйте біографію перед тим, як наймати працівників, які матимуть доступ до конфіденційної інформації.

2. Вимагайте від кожного з ваших нових працівників підписання договору щодо дотримання стандартів захисту персональних даних та забезпечення їх безпеки. Впевніться, що вони розуміють, що дотримання плану захисту та безпеки даних вашої компанії є суттєвою частиною їх обов’язків. Регулярно нагадуйте працівникам про політику вашої компанії та будь-які законодавчі вимоги зберігання відомостей про клієнтів у захищеному місці.

3. Майте інформацію щодо того, хто з працівників має доступ до персональних даних клієнтів. Звертайте особливу увагу на такі дані, як номери соціального захисту та номери рахунків. Обмежуйте доступ до персональних даних працівників.

4. Ваша компанія повинна мати процедури, які забезпечуватимуть, щоб працівники, які звільняються або переходять до іншого підрозділу, не мали доступу до конфіденційної

інформації. Обмежуйте термін дії їх паролів, зберігайте в безпечному місці ключі та ідентифікаційні відомості, як частину звичайного режиму перевірки.

5. Розповідайте працівникам про політику компанії стосовно дотримання захисту та безпеки даних. Впевніться, що ваша політика донесена до працівників, що мають доступ до персональних даних з дому чи іншого місця.

6. Попереджайте працівників про телефонний фішинг[6]. Навчайте їх бути обережними з незнайомими людьми, що телефонують, вимагають номер рахунку для оброблення замовлення або які запитують контактні дані клієнтів чи ваших працівників. Зробіть стандартною практикою подвійну перевірку шляхом контакту з компанією, що використовує номер телефону, який ви знаєте.

7. Вимагайте, щоб працівники повідомляли вас негайно, якщо є небезпека порушення захисту даних, наприклад, втрата чи крадіжка ноутбуку.

8. Впровадьте дисциплінарне покарання за порушення заходів безпеки.

3.4. Практика щодо безпеки підрядників та постачальників послуг

Практика компанії щодо безпеки даних залежить від людей, які впроваджують її, включаючи підрядників та постачальників послуг.

1. Перед тим як ви передасте будь-які функції вашого бізнесу (веб-хостинг, клієнтські кол-центри обробки даних), вивчіть практику їх захисту і порівняйте з вашими стандартами.

2. Під час укладання контрактів з вашими постачальниками послуг звертайте увагу на положення щодо безпеки даних в таких контрактах.

3. Вимагайте, щоб постачальники послуг повідомляли вам про кожний випадок порушення безпеки, що стався, навіть якщо такий випадок не завдав фактичної шкоди.

Стаття 4. Видалення даних

Те, що для вас купа сміття, може бути золотою знахідкою для грабіжника даних. Залишення рахунків по кредитних картках або паперів чи дисків з персональними даними в ящику для сміття посилює можливість вчинення злочину і піддає клієнтів ризику викрадення їх персональних даних. Шляхом правильного використання конфіденційної інформації ви забезпечуєте, щоб її не було прочитано чи відновлено.

1. Впроваджуйте практику, яка необхідна для запобігання несанкціонованому доступу до персональних даних, їх обробці, використанню та несанкціонованому поширенню.

2. Знищуйте паперові записи, використовуючи спеціальне обладнання та спалюючи їх. Зробіть так, щоб обладнання для подрібнення паперу не було доступне на робочих місцях.

3. При ліквідації старих комп’ютерів та засобів зберігання даних використовуйте програми для стирання даних. Вони недорогі та більш результативні при перезапису жорсткого диску, здійснюючи це таким чином, щоб файли неможливо було більше відновити. Видалення файлів, використовуючи клавіатуру або команди миші, як правило неефективне тому, що файли можуть продовжувати існування на жорсткому диску і можуть були відновлені.

4. За можливістю, впевніться, що працівники, які працюють вдома, дотримуються тих же процедур з ліквідації відомостей і даних щодо конфіденційної інформації, що зберігаються на їх комп’ютерах та засобах зберігання даних.

5. Якщо використовуєте кредитну історію клієнтів для цілей вашої діяльності, на вас поширюються правила ліквідації даних Федеральної торгової комісії.

Стаття 5. Попереднє планування

Здійснення заходів з захисту даних, що знаходяться у вашому розпорядженні, з метою запобігання порушенням системи безпеки може зайняти довгий період часу. Тим не менш, порушення можуть траплятися. Нижченаведеними способами ви можете зменшити такий вплив на вашу діяльність, ваших працівників та ваших клієнтів:

[6] Різновид Інтернет-шахрайства, вивідування інформації, що дає змогу здійснити викрадення персональних даних.

1. З метою реагування на випадки порушення захисту та безпеки майте відповідний план реагування. Призначте одного з ваших працівників головним по координації і впровадженню відповідного плану.

2. Якщо до вашого комп’ютера було здійснено несанкціонований доступ, відключіть його негайно від локальної мережі або Інтернету.

3. Одразу ж розслідуйте випадки порушення захисту чи безпеки та вживайте необхідних заходів блокування слабких місць в системі захисту даних або загроз безпеці персональних даних.

4. Визначтесь, кого потрібно повідомити, як всередині вашої організації, так і зовнішні інстанції, якщо трапився випадок порушення безпеки даних. Можливо, вам необхідно буде повідомити покупців, правоохоронні органи, клієнтів, кредитні бюро та інші компанії, на яких може вплинути таке порушення. Окрім того, багато регулюючих органів держав та федеральних банків мають закони або посібники щодо порушення захисту даних.

Використана література

1. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 р. № 108 : у кн. “Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних” : посіб. / [В. Брижко, М. Швець та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

2. Захист персональних даних в сфері Інтернет речей / О. Баранов, В. Брижко // Інформація і право. – № 2(17)/2016. – С.85-91.

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

4. Конвергенція новітніх технологій : стан і перспективи змін у інформаційних відносинах / В. Брижко, В. Фурашев // Інформація і право. – № 1(20)/2017. – С. 58-67.

5. Защита персональных данных в Интернете в странах Европейского Союза. – Режим доступу : https://ru.wikipedia.org

6. 4 преграды на пути Интернета вещей. – Режим доступа : http://ubr.ua/ukraine-and-world/technology/4-pregrady-na-puti-interneta-veshei-362374

7. S. Chen et al. A Vision of IP : Applications, Challenges and Opportunities With China Perspective IEEE / Internet of Things Journal, vol. 1, No. 4. – Pp. 349-359. – August 2014. – Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=6851114

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

9. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижко, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ “Видавничий дім “АртЕк”, 2017. – 226 с.

10. On the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) : Reglament (EU) 2016/679 of the European Parlament and of the Council, of 27 April 2016 / Регламент (ЄС) 2016/679 від 27.04.16 р. – Available at: http://eur-lex.europa.eu/legal-content /EN/ TXT/HTML/?uri=CELEX:32016 R0679&from= EN

11. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних : зб. документів ; [неоф. пер. з англ. І. Майстренко] ; за ред. В. Брижко ; передмова В. Пилипчука. – (НДІ інформатики і права Національної академії правових наук України). – К. : ТОВ “Видавничий дім “АртЕк”, 2018. – 180 с.

12. Корпоративні механізми (Кодекси поведінки) у сфері захисту персональних даних : в кн. “Інформаційне право та правова інформатика у сфері захисту персональних даних” / [В. Брижко, М. Швець та ін.] ; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2005. – 451 с. – С. 27-30.

13. Charter of Fundamental Rights of the European Union, of 7 December 2000. – Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12012P%2FTXT

14. Подходы к защите персональных данных в ЕС и США. – Режим доступу : https://euroua.com/humrights/violations/1723-podkhody-k-zashchite-personalnykh-dannykh-v-es-i-ssha

15. – Режим доступу : http://itc.ua/news/senat-ssha-podderzhal-zakonoproekt-kotoryiy-pozvolit-internet-provayderam-ispolzovat-personalnyie-dannyie-polzovateley-bez-ih-soglasiya

16. До питання е-торгівлі та захисту персональних даних / В. Брижко // Правова інформатика. – № 1(13)/2007. – С. 14-28; Економічні та правові аспекти проблеми захисту персональних даних / В. Брижко // Правова інформатика”. – № 1(29)/2011. – С. 25-35.

17. Послугу з e-mail розсилки існуючої бази клієнтів. – Режим доступу : https://kiev.all.biz/baza-mobilnyh-nomerov-kieva-ukraina-bazy-klientov-g5081769

18. Економічний аспект захисту персональних даних у контексті права власності на інформацію / В. Брижко // Правова інформатика. – № 1(9)/2006. – С. 47-57.

19. Три скользких момента в законе ЕС о защите персональных данных. – Режим доступу : http://www.aif.uasociety/social/tri_skolzkih_momenta_v_zakone_es_o_zashchite_personalnyh_dannyh

20. Защита персональных данных / [А. Баранов, В. Брыжко, Ю. Базанов]. – К. : Национальное агентство по вопросам інформатизації при Президенте Украины, ВАТ КП ОТІ, 1998. – 128 с. – С. 41-42, 84.

21. Права человека и защита персональных данных / [А. Баранов. В. Брыжко, Ю. Базанов]. – Харьков : Фолио, 2000. – 280 с. – С. 169-176, 220-221, 233. – (Финансовая помощь и содействие в издании Харковской правозащитной группы и Национального фонда поддержки демократии (США).

22. 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. – С. 131.

23. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В. Брыжко. – К. : ТОВ “ПанТот”, 2012 р. – 304 с. – (Про захист персональних даних. – С. 117-130).

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

Pylypchuk Volodymyr, Bryzhko Valery, 2016. PRIVACY AND HUMAN SECURITY IN THE PROTECTION OF PERSONAL DATA. Social and Human Sciences. Polish-Ukrainian scientific journal, 04(12). – Available at: http://sp-sciences.io.ua/s2596466/pylypchuk _volodymyr_ bryzhko_valery_2016._privacy_and_human_security_in_the_protection_of_personal_data._social_and_human_sciences._polish-ukrainian_scientific_journal_04_12_ (accessed 08 January 2017)

25. – Режим доступу : http://www.eurasialegal.info/index.php?option=com_content&view=article&id=5192:2017-02-20-06-48-58&catid=314:2015-02-05-10-21-50

26. Забезпечення захисту персональних даних у комерційних організаціях : за матеріалами посібника для бізнесу Федеральної торгової комісії США / [пер. з англ. Віри Брижко] ; за ред. В.М. Брижко. – Режим доступу : //www.ftc.gov/bcp/edu/pubs/business/ idtheft/bus69.pdf

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

УДК 341: 316.774: 070.13

ЗАБАРА І.М., *кандидат юридичних наук,* доцент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка

МІЖНАРОДНО-ПРАВОВЕ РЕГУЛЮВАННЯ ВИКОРИСТАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ РЕСУРСІВ В УМОВАХ НАДЗВИЧАЙНИХ СИТУАЦІЙ: ДО ДВАДЦЯТИРІЧЧЯ КОНВЕНЦІЇ ТАМПЕРЕ 1998 РОКУ

***Анотація**. У статті досліджуються питання міжнародно-правового регулювання діяльності з використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій. Автор акцентує увагу на комунікаційній складовій міжнародно-правової проблематики діяльності суб’єктів в умовах надання гуманітарної допомоги. Автор розглядає передумови, сферу регулювання, засади і умови міжнародно-правового співробітництва з надання телекомунікаційних ресурсів для пом’якшення наслідків стихійних лих та здійсненні операцій з надання допомоги. Аналізуються проблемні питання базових засад міжнародно-правового режиму сучасних міжнародних комунікаційних відносин у сфері надання допомоги у випадку стихійних лих і надзвичайних ситуацій..*

***Ключові слова**: телекомунікації, телекомунікаційні ресурси, телекомунікаційна допомога, міжнародно-правовий режим, міжнародно-правові відносини.*

***Summary.** The article deals with the issues of international legal regulation of activity on the use of telecommunication resources in the conditions of emergency situations. The author focuses on the communication component of the international legal issues of the subjects' activities in the provision of humanitarian assistance. Examines the preconditions, the scope of regulation, the principles and conditions of international legal cooperation for the provision of telecommunication resources for mitigating the effects of natural disasters and the implementation of assistance operations. The article analyzes the problematic issues of the basic principles of the international legal regime of modern international communication relations in the field of assistance in the event of natural disasters and emergencies.*

***Keywords**: telecommunications, telecommunication resources, telecommunication assistance, international legal regime, international legal relations.*

***Аннотация**. В статье исследуются вопросы международно-правового регулирования деятельности по использованию телекоммуникационных ресурсов в условиях чрезвычайных ситуаций. Автор акцентирует внимание на коммуникационной составляющей международно-правовой проблематики деятельности субъектов в условиях предоставления гуманитарной помощи. Автор рассматривает предпосылки, сферу регулирования и условия международно-правового сотрудничества по предоставлению телекоммуникационных ресурсов для смягчения последствий стихийных бедствий и осуществления операций по оказанию помощи. Анализируются проблемные вопросы международно-правового режима современных международных коммуникационных отношений в сфере оказания помощи в случае стихийных бедствий и чрезвычайных ситуаций.*

***Ключевые слова:** телекоммуникации, телекоммуникационные ресурсы, телекоммуникационная помощь, международно-правовой режим, международно-правовые отношения.*

Постановка проблеми та актуальність дослідження. 18 червня 1998 року на міжнародній конференції в місті Тампере (Фінляндія), було прийнято *Конвенцію про надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій із надання допомоги* (далі, офіційна скорочена назва – Конвенція Тампере) [1].

Прийняття зазначеної Конвенції виступило свідченням того факту, що світове співтовариство в питанні регламентації діяльності у випадку стихійних лих та в рамках концепції “міжнародного права катастроф” наблизилось до значно нового рівня правового регулювання захисту і надання допомоги, покликаних зменшити число людських жертв, страждань людей, масштабів шкоди майну та навколишньому середовищу.

Конвенція Тампере стала визначальною універсальною конвенцією, яка фактично розпочала новий, третій етап розвитку регламентації міжнародно-правової співпраці на випадок стихійних лих, а саме – період після 1990 року [2, с. 12], що було обумовлено, “по-перше, еволюцією міжнародно-правової думки щодо регламентації міжнародних відносин, пов’язаних із діяльністю на випадок стихійних лих, та по-друге, етапами становлення принципів та норм, які тим чи іншим чином регулюють досліджувані відносини” [2, с. 12].

У загальному контексті надання гуманітарної допомоги у випадку стихійних лих, Конвенція Тампере визначає і забезпечує:

- міжнародно-правову основу для розгортання і використання електрозв’язку при наданні міжнародної гуманітарної допомоги,

- міжнародно-правову основу гарантованого оперативного надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій з надання допомоги,

- міжнародно-правову основу (своєчасного, оперативного, повного та достовірного) отримання, обміну і поширення інформації про небезпечні природні явища, небезпеку для здоров’я людей і стихійні лиха, а також

- сприяє міжнародному співробітництву в області зменшення масштабів впливу стихійних лих.

Разом з тим, Конвенція Тампере містить і низку положень, що підлягають подальшій деталізації, оскільки перед світовим співтовариством постають нові завдання, визначаються нові пріоритети і висуваються нові вимоги.

Поряд з іншими питаннями, важливим є визначення і узагальнення базових засад міжнародно-правового режиму сучасних міжнародних відносин в сфері використання телекомунікаційної допомоги і телекомунікаційних ресурсів. Вартою, на нашу думку, буде і увага до концептуальних підходів, що пропонуються в рамках міжнародних організацій.

Результати аналізу наукових публікацій свідчить про те, що коло проблемних питань, висвітлених у роботах Д. Александера, П.Н. Бірюкова, П. Волкера, Й. Дінстайна, В.А. Євсєгнєєва, К. Жоржа, В.В. Ласаускайте, І.І. Лукашука, А.І. Микульшина, Б. Морза, П. Макалістер-Сміта, Дж. Потики, Л.Р. Сивко, Д. Фідлера, Р. Хардкасла, Дж. Хатчинсона, А. Чуа, П. Уокера, Є.Т. Усенка, Г.Г. Шинкарецької та інших вчених є доволі широким. Серед розглянутих авторами – питання співробітництва держав у сфері подолання наслідків стихійних лих, міжнародно-правової регламентації відносин, пов’язаних із діяльністю на випадок стихійних лих, питання міжнародно-правового режиму діяльності з надання гуманітарної та іншої допомоги. Разом з тим, враховуючи різноманітність розглянутої авторами тематики, вартими окремого розгляду є і питання щодо сучасних теоретичних і практичних підходів до правових засад надання телекомунікаційної допомоги і телекомунікаційних ресурсів, зокрема на тлі достатньо нешорокого кола наукових робіт із цього аспекту правовідносин.

Важливою, на нашу думку, є і позиція Комісії міжнародного права ООН та Міжнародної федерації організацій Червоного Хреста та Червоного Півмісяця.

Метою статті є визначення і узагальнення базових засад міжнародно-правового режиму сучасних комунікаційних відносин в сфері використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій.

Виклад основних положень. Проблематика міжнародно-правового регулювання надання телекомунікаційних ресурсів для подолання наслідків стихійних лих, що здійснюється у в рамках гуманітарної допомоги, посідає окреме місце.

Прийнята *Конвенція Тампере про надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій із надання допомоги 1998 р.* [1] стала результатом Першої міжурядової конференції з надзвичайних ситуацій електрозв’язку “ICET-98”. Конвенція Тампере була прийнята 60 державами і ратифікована 49, набула чинності 8 січня 2005 року [3].

Прийняття зазначеної Конвенції виступило *з одного боку* – показником спільного бачення міжнародного співтовариства проблематики щодо численних ситуацій з надання гуманітарної допомоги у випадках стихійних лих і надзвичайних ситуацій і, окремо – питаннями їхнього міжнародно-правового регулювання, а *з іншого боку* – поштовхом у розвитку міжнародно-правового регулювання відносин, пов’язаних із забезпеченням передачі інформації, а також наданням та використанням зв’язку та телекомунікаційних ресурсів за надзвичайних умов (техногенних та природніх катастроф).

Таке комплексне розв’язання було викликано низкою чинників. Зокрема тими, що склались переважно у період до дев’яностих років XX сторіччя і, на сьогодні, характеризуються наступним:

- відсутністю системного підходу до діяльності держав та її міжнародно-правового регулювання на випадок стихійних лих;
- відсутністю універсального договірного і інституційного механізмів міжнародного співробітництва у здійсненні операцій із надання допомоги і подоланні наслідків стихійних лих. Позитивним для розвитку міжнародно-правового регулювання використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій стало прийняття Конвенції про створення та Статут Міжнародного союзу допомоги (1927 р.), а також діяльність першої і фактично єдиної міжурядової організації – Міжнародного союзу допомоги, що однак не набула широкої підтримки;
- початковим розвитком двостороннього, а з часом – і регіонального співробітництва переважно на умовах укладання угод ad hoc, між різними суб’єктами (державами і міжнародними урядовими і міжнародними неурядовими організаціями) з питань діяльності у випадках стихійних лих, надання допомоги і подоланні наслідків;
- поступовим зростанням ролі міжнародних неурядових гуманітарних організацій у наданні допомоги та подоланні наслідків стихійних лих;
- появою окремих міжнародно-правових досліджень з проблематики надання гуманітарної допомоги у випадках стихійних лих і надзвичайних ситуацій;
- розумінням численних проблем і намаганням держав розширити договірну базу і заснувати міжнародну організацію.

Разом з тим, у період після 1990 року, підвищена увага світового співтовариства до категорії комунікації і комунікаційної діяльності, у зв’язку із появою і стрімким розвитком інформаційно-комунікаційних технологій, викликала нове бачення, наповнення і розуміння проблематики з використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій зокрема, у разі стихійних лих.

Йдеться про міжнародне співробітництво і міжнародно-правове регулювання використання телекомунікаційних ресурсів у певних, визначених ситуаціях, а саме – у

разі серйозних порушень функціонування суспільства, які створюють загрозу життю і здоров’ю людей, майну або навколишньому середовищу, незалежно від того, чи викликані вони природними силами або техногенними аваріями, виникли раптово або у результаті певного процесу.

У рамках міжнародно-правового регулювання, важливими для розгляду варто виокремити наступні питання:

1. Передумови розвитку проблематики;
2. Сфера регулювання і особливості термінології;
3. Засади і умови міжнародно-правового співробітництва.

1. ***Передумовами розвитку проблематики з міжнародно-правового регулювання надання телекомунікаційних ресурсів в умовах надзвичайних ситуацій*** виступила низка чинників, які спрямували зусилля світового співтовариства на розробку відповідних положень. Серед головних виступили:

– визнання того факту, що “масштаби, складність, частота і вплив стихійних лих збільшуються швидкими темпами” (п. 1 Преамбули) [1]; ці процеси супроводжуються стражданнями жертв стихійних лих та надзвичайних ситуацій, загибеллю людей, масовим переміщенням людей і матеріальними руйнаціями (п. 9 Преамбули Резолюції ГА ООН 51/194) [7], (п. 2) [4];

– занепокоєння масштабним “впливом стихійних лих на комунікаційні системи і потоки інформації” (п. 6 Преамбули) [1],

– розуміння “важливої ролі телекомунікацій у справі пом’якшення наслідків від стихійних лих і надзвичайних ситуацій та наданні допомоги” (п. 13 Преамбули) [1], а також визнання “важливої ролі мовлення у поширенні точної інформації про стихійні лиха” (п. 4 Преамбули) [1];

– потреба “установ з надання гуманітарної та іншої допомоги у надійних телекомунікаційних ресурсах для виконання їх задач, а також забезпеченні безпеки персоналу з надання гуманітарної та іншої допомоги” (п. 2, п. 3 Преамбули) [1];

– бажання “забезпечити наявність надійних, швидко доступних телекомунікаційних ресурсів для пом’якшення наслідків стихійних лих і здійснення операцій з надання допомоги за підтримки держав, державних і недержавних установ” (п. 20, п.19 Преамбули) [1];

– усвідомлення і переконання у тому, що “ефективне, своєчасне розгортання телекомунікаційних ресурсів і швидкі і ефективні потоки точної і правдивої інформації мають надзвичайно важливе значення для зменшення кількості людських жертв, страждань людей і шкоди майну і навколишньому середовищу, у результаті стихійних лих” (п. 5 Преамбули) [1];

– наголошення на “особливих потребах найменш розвинутих держав світу у технічній допомозі у (питанні) розвитку телекомунікаційних ресурсів для пом’якшення наслідків стихійних лих та здійсненні операцій з надання допомоги” (п.1, п.7 Преамбули) [1] [4];.

– підтвердження “абсолютного пріоритету, що надається аварійним рятівним комунікаційним засобам, що відображено у більш ніж п’ятдесяти міжнародних нормативних документах, у тому числі у Статуті Міжнародного союзу електрозв’язку” (п. 8, п.10 Преамбули) [1; 5];

– розвиток “ReliefWeb” як глобальної системи інформації гуманітарного характеру з метою поширення обміну і достовірної і своєчасної інформації про стихійні лиха і надзвичайні ситуації (п. 13 Резолюції 51/194) [7], п.17 Преамбули) [1];

– бажання сприяти міжнародному співробітництву із пом’якшення наслідків стихійних лих, враховуючи історію міжнародного співробітництва і координації пом’якшення наслідків стихійних лих, надання допомоги, рятування людей при використанні телекомунікаційних ресурсів (п. 21, п. 9, п. 12, п. 14, п. 15, п. 17 Преамбули) [1], (Резолюція ГА ООН №51/194) [7].

2. ***Сфера регулювання і особливості термінології***. Для розгляду проблематики міжнародно-правового регулювання відносин з (a) використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій та (б) сприяння міжнародному співробітництву при наданні телекомунікаційних ресурсів для пом’якшення наслідків лих і надання допомоги, вартим, на нашу думку, є стислий попередній розгляд термінології – як за визначенням (a) небезпечних явищ (подій), (b) суб’єктного складу, так і (c) окремих понять у сфері телекомунікаційних відносин. Це цілком відповідатиме сучасним міжнародно-правовим поглядам, висловленим в рамках Комісії міжнародного права ООН [6] (далі – КМП ООН), що охоплюють питання:

- *ratione materiae* (в тому числі поняття лиха та його класифікація),
- *ratione personae* (діяльність державних і недержавних суб’єктів),
- *ratione temporis* (дії до лиха, під час лиха і після нього).

(a) Розгляд термінології щодо небезпечних явищ (подій) потрібен для розуміння принципового питання – на які саме випадки поширюється надання телекомунікаційних ресурсів та телекомунікаційної допомоги.

Зауважимо, що питання щодо визначення і характеристики небезпечних явищ, за яких передбачається надання, в рамках гуманітарної допомоги, зокрема – телекомунікаційної допомоги, виступало і залишається одним із важливих, принципових і дискусійних протягом доволі тривалого часу.

Тому, для характеристики цих явищ конвенційно було визначено кілька понять, зокрема “лихо”, “небезпечне природнє явище”, “небезпека для здоров’я людей”, “операції з надання допомоги”, “пом’якшення наслідків лих”.

Ключовим виступає поняття “*лихо*” (англ. - disaster, icп. - catastrofe, рос. - бедствие, фр. - catastrophe), що означає “серйозне порушення функціонування суспільства, яке створює серйозну, широку загрозу для життя і здоров’я людей, майна або навколишнього середовища, незалежно від того, чи викликано воно аварією, силами природи або діяльністю людини і виникло раптово або у результаті складного, тривалого процесу” (п. 6 ст. 1) [1].

Саме в разі класифікації події у якості “лихо” – можливим є надання телекомунікаційних ресурсів і допомоги на умовах Конвенції Тампере.

Інші конвенційні терміни – “небезпечне природнє явище”, “небезпека для здоров’я людей”, “операції з надання допомоги”, “пом’якшення наслідків лих” – покликані відповідно розкрити поняття заходів, явищ, процесів та діяльності, що спрямовані на подолання або зменшення впливу лиха.

Зауважимо, що визначені Конвенцією Тампере терміни щодо небезпечних явищ (подій) виступають результатом компромісу між державами, оскільки, як зазначає КМП ООН, виступають “найбільш відповідним орієнтиром” (п. 44), про що зазначалось у її *“Другій доповіді про захист людей у випадку лиха”* 2009 р. [6]. Роботи із вдосконалення термінології продовжуються, про що свідчить як аналіз низки регіональних угод, так і доктринальне визначення ключового поняття ” “лиха” (п. 45) запропоноване самою КМП ООН, та його характеристики (пп. 46-49) [6]. Зокрема, за пропозицією КМП ООН – “лихо” означає “серйозне порушення функціонування суспільства, що не включає

збройний конфлікт, яке призводить до значних масових людських, матеріальних і екологічних втрат” [6].

Визначення термінології щодо небезпечних явищ (подій) виступило суттєвим внеском у питання міжнародно-правового регулювання надання телекомунікаційних ресурсів і телекомунікаційної допомоги у випадку стихійних лих.

(b) Звернення до термінології щодо суб’єктного складу є важливим з тієї причини, що у операціях з (а) пом’якшення або ліквідації наслідків лих, (б) надання телекомунікаційних ресурсів, (в) телекомунікаційної і гуманітарної допомоги крім держав, беруть участь і інші суб’єкти – міжнародні неурядові організації, приватні і корпоративні утворення, що стало типовим у правовідносинах з надання гуманітарної допомоги у випадках стихійних лих.

Для характеристики суб’єктного складу обрано такі терміни, як “держава-учасниця, що надає допомогу”, “держава-учасниця, що запитує допомогу”, “неурядова організація” (визначається як будь-яка організація, включаючи приватні і корпоративні утворення, що не є державними або урядовими або міжурядовими організаціями”) (п. 10 ст. 1) [1], “недержавне утворення” (розглядається як будь-яке утворення, включаючи неурядові організації і рух Червоного Хреста і Червоного Півмісяця) (п. 11.ст. 1) [1].

Разом з тим, досить важливо звернути увагу і на нового суб’єкта правовідносин – “Координатора надзвичайної допомоги Організації Об’єднаних Націй”.

(c) Крім термінології щодо небезпечних явищ, суб’єктного складу, визначено і окремі поняття у сфері телекомунікаційних відносин, зокрема, поняття “телекомунікації”, “телекомунікаційні ресурси”, “телекомунікаційна допомога”.

Варто, на нашу думку, звернутись до їх конвенційного визначення. Зокрема, “*телекомунікації* – означають будь-яку передачу, трансляцію або приймання знаків, сигналів, письмових матеріалів, зображень, звуків або відомостей будь-якого роду дротами, радіо, оптиковолокном або за допомогою іншої електромагнітної системи” (п. 15 ст. 1) [1]. Зауважимо, що це визначення у повному обсязі кореспондує поняттю *“електрозв’язок”*, визначеному для усієї відповідної діяльності під егідою Міжнародного союзу електрозв’язку (п. 1012 Додатку Статуту МСЕ) [5].

Разом з тим, термін “*телекомунікаційні ресурси* – означає персонал, обладнання, матеріали, інформацію, професійну підготовку, радіочастотний діапазон, мережу або трансляційні заходи або інші ресурси, необхідні для телекомунікацій” (п. 14 ст. 1) [1]. Таке розширене поняття “телекомунікаційних ресурсів” покликане охопити якомога більше елементів з метою надання широкого спектру допомоги.

У свою чергу, конвенційно визначено, що “*телекомунікаційна допомога* – означає надання телекомунікаційних або інших ресурсів або підтримки, покликаної сприяти використанню телекомунікаційних ресурсів” (п.13 ст.1) [1].

Зазначимо, що поєднання у Конвенції Тампере широкого кола визначених випадків надання телекомунікаційної допомоги і визначення відповідної термінології щодо небезпечних явищ, суб’єктного складу та окремих понять у сфері телекомунікаційних відносин, виступило значним чинником у питаннях сприяння міжнародному співробітництву для пом’якшення наслідків лих.

3. ***Засади і умови міжнародно-правового співробітництва при наданні телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій із надання допомоги*** виокремлюють це питання в рамках більш широкого питання – міжнародно-правового співробітництва з надання гуманітарної допомоги за стихійних лих.

Надання телекомунікаційної допомоги, відповідно до положень Конвенції Тампере, відбувається згідно з принципами і нормами міжнародного права, за певною процедурою і з дотриманням визначених умов.

Метою співробітництва (між державами, міжурядовими організаціями і недержавними утвореннями) є “сприяння використанню телекомунікаційних ресурсів для пом’якшення наслідків [стихійних] лих і надання допомоги” (п. 1 ст. 3) [1]. Таке використання ресурсів, відповідно до положень Конвенції Тампере, має комунікаційну і інформаційну складові.

Зокрема, комунікаційна складова передбачає:

а) “розгортання наземного і супутникового телекомунікаційного обладнання…” (п. 2a ст. 3);

б) “надання швидкої телекомунікаційної допомоги…” (п. 2c ст. 3);

в) “встановлення і експлуатацію надійних, гнучких телекомунікаційних систем…” (п. 2d ст. 3);

Разом з тим, інформаційна складова передбачає:

г) “прогнозування, спостереження і *отримання інформації* про небезпечні природні явища, небезпеку для здоров’я людей і лиха” (п. 2a ст. 3);

д) “*обмін інформацією* про небезпечні природні явища, загрози для здоров’я людей і лихах між учасниками відносин, а також *поширення такої інформації* серед населення …” (п. 2b ст. 3).

Процедура, умови, права і обов’язки сторін щодо телекомунікаційної допомоги охоплюють, за умовами Конвенції Тампере, принципові питання зокрема, запиту і отримання згоди на її надання, початку її надання, вірогідної компенсації, її припинення та можливі правові наслідки.

За погодженою процедурою, телекомунікаційна допомога для пом’якшення наслідків стихійних лих надається виключно на запит держав (п. 1 ст. 4) [1]. Для цього “держава-учасниця, що запитує допомогу”, може звернутись безпосередньо до іншої держави учасниці Конвенції, або до Координатора надзвичайної допомоги Організації Об’єднаних Націй (далі – координатор операцій). І держава, і координатор операцій взаємно повідомляють один одного і поширюють інформацію серед інших держав (п. 1 ст. 4).

Держава, що запитує телекомунікаційну допомогу зазначає розмір, характер і заходи необхідної допомоги (п.2 ст.4) [1]. У свою чергу *“держава-учасниця, що надає допомогу”*, визначає і повідомляє (безпосередньо, або через координатора операцій) про можливість її надання, а також розміри, терміни, умови, обмеження і можливу вартість такої допомоги (п. 3 ст .4).

Водночас, кожна з держав, що у свою чергу, вирішила надати телекомунікаційну допомогу, інформує якомога скоріше координатора операцій (п. 4 ст. 4).

За умовами Конвенції Тампере, телекомунікаційна допомога не надається без згоди держави, що запитує допомогу. Крім того держава, що запитує допомогу зберігає за собою право відхилити усю або частину телекомунікаційної допомоги, посилаючись на чинне внутрішньодержавне законодавство або політику (п. 5 ст. 4) [1].

За будь-якими державами зберігається право, у відповідності з внутрішньодержавним законодавством, спрямовувати, контролювати і координувати телекомунікаційну допомогу, що надається на підставі Конвенції, в межах її території або здійснювати такий контроль за такою допомогою (п. 8 ст. 4).

За державами, що запитують допомогу, визнається право запитувати телекомунікаційну допомогу безпосередньо у недержавних утворень і міжурядових

організацій. У свою чергу, за недержавними утвореннями і міжурядовими організаціями визнається право надавати телекомунікаційну допомогу державам, що її запитують (п. 6 ст. 4).

Недержавні утворення і міжурядові організації не можуть виступати в якості суб’єкта, що запитує допомогу, і не можуть просити про її надання на підставі Конвенції (п. 7 ст. 4).

Держава-учасниця, що запитує допомогу, в міру своїх можливостей, створює умови і надає місцеві послуги для належного і ефективного надання телекомунікаційної допомоги (швидке ліцензування або звільнення від ліцензування телекомунікаційного обладнання, його захист) (п. 2, 3 ст. 5) [1].

Держави-учасниці, по можливості, у відповідності із внутрішньодержавним законодавством, усувають регламентуючі бар’єри на шляху використання телекомунікаційних ресурсів (зокрема положення, що обмежують імпорт або експорт телекомунікаційного обладнання; використання телекомунікаційного обладнання або радіочастотного діапазону; обмеження пересування персоналу, що працює з телекомунікаційним обладнанням; положення щодо ввезення, вивезення і провезення через територію телекомунікаційних ресурсів (ст. 9).

Використання обладнання і матеріалів, наданих у рамках допомоги, не впливає на право власності. Держава-учасниця, що запитує допомогу, забезпечує швидке повернення такого обладнання, матеріалів та майна тій державі, що надає допомогу (п. 4 ст. 5).

Держава-учасниця, що запитує допомогу, не дає розпоряджень щодо розгортання або використання телекомунікаційних ресурсів для цілей, безпосередньо не пов’язаних із прогнозуванням стихійних лих, підготовкою до них, прийняттям заходів у відповідь, спостереженням, пом’якшенням їх наслідків і наданням допомоги під час або після стихійних лих (п. 5 ст. 5) [1].

Особи і організації, що надають телекомунікаційну допомогу або іншим чином сприяють використанню телекомунікаційних ресурсів, зобов’язані поважати закони і правила цієї держави. Такі особи і організації також зобов’язані не втручатись у внутрішні справи держави, на територію якої вони прибули (п. 7 ст. 5).

“Держава, що запитує допомогу” і “держава що надає допомогу” можуть у будь-який час припинити надання і отримання телекомунікаційної допомоги шляхом письмового повідомлення. Далі, за процедурою, держави розпочинають консультації для належного і швидкого припинення допомоги, враховуючи наслідки такого припинення допомоги, з точки зору небезпеки для життя людей і операцій, що здійснюються з надання допомоги від стихійних лих (п. 1 ст. 6) [1].

Держава, що звертається з проханням про припинення телекомунікаційної допомоги, повідомляє про це координатора операцій, який сприяє їй (п. 3 ст. 6).

Держави можуть обумовити надання телекомунікаційної допомоги задля пом’якшення наслідків лих отриманням згоди сплатити або відшкодувати відповідні витрати (п. 1 ст. 7).

При визначенні доцільності сплати або відшкодування за надання телекомунікаційних послуг, держави беруть до уваги, разом із іншими, наступні чинники: a) принципи ООН щодо гуманітарної допомоги; b) характер лиха, небезпечного природного явища або небезпеки для здоров’я людей; c) вплив або потенційний вплив стихійного лиха; d) місце походження стихійного лиха; e) район, що потерпів або може потерпіти в результаті стихійного лиха; f) випадки стихійних лих у минулому і вірогідність лиха у майбутньому у потерпілому районі; g) здатність кожної

держави, охопленої стихійним лихом, небезпечним природним явищем або небезпекою для здоров’я людей, підготуватись до таких явищ або прийняти відповідні заходи; h) потреби держав, що розвиваються (п. 8 ст. 7) [1].

Такі самі умови щодо відшкодування поширюються і на випадки, коли телекомунікаційну допомогу надають недержавні утворення або міжурядові організації в разі, якщо держава погоджується на це (п. 9 ст. 7).

В разі, якщо надання телекомунікаційної допомоги обумовлено оплатою або відшкодуванням витрат, то вони здійснюються негайно, після прохання держави, що надає допомогу (п. 6, п. 7 ст. 7) [1].

Кожна держава, на прохання іншої, тією мірою, якою це допускається внутрішньодержавним законодавством, сприяє ввезенню, вивезенню і транзиту через свою територію персоналу, обладнання, матеріалів і інформації, пов’язаних із використанням телекомунікаційних ресурсів для пом’якшення наслідків стихійних лих і надання допомоги (п. 4 ст. 9) [1].

За загальними умовами, для сприяння використанню телекомунікаційних ресурсів задля пом’якшення наслідків стихійних лих і надання допомоги, держави можуть:

- укладати додаткові багатосторонні або двосторонні угоди і домовленості (п. 3 ст. 3),
- створювати механізми для навчання поводженню з обладнанням і його застосуванню (п. 5 ст. 3),
- [впроваджувати] ознайомчі курси з питань розробки, проектування і створення телекомунікаційних служб для попередження, моніторингу і пом’якшення наслідків стихійних лих (п. 5 ст. 3).

При цьому держави, за допомогою міжнародних організацій, звертаються до:

(a) практики розробки і використання типових угод (п. 4a ст. 3),

(b) найбільш ефективної практики (п. 4b ст. 3),

(c) іншої відповідної інформації з використанням електронних засобів і відповідних механізмів (п. 4b ст. 3),

(d) розробки, застосування і підтримки процедур та систем збору і поширення інформації (п. 4c ст. 3) [1].

Такими виступають узагальнені базові засади міжнародно-правового режиму сучасних комунікаційних відносин в сфері використання телекомунікаційних ресурсів в умовах надзвичайних ситуацій.

Разом з тим, заслуговує на увагу двадцятирічний досвід застосування Конвенції Тампере, а також діяльність міжнародних організацій універсального характеру з її вдосконалення.

Провідну і координуючу роль відіграє ООН та її органи, що уповноважені сприяти міжнародному співробітництву в області гуманітарної допомоги у випадку стихійних лих. Координуючими і спрямовуючими діяльність виступають:

- Всесвітні конференції ООН із зменшення небезпек від лиха. Прийняті *“Хіогська декларація” і “Хіогська рамочна програма дій на 2005 – 2015 роки: створення потенціалу протидії лихам на рівні держав і громад”* виступили поштовхом для продовження відповідної діяльності на період після 2015 р.;
- Глобальна платформа ООН з дій із зменшення небезпек від лиха;
- Платформа ООН з використання космічної інформації для попередження і ліквідації надзвичайних ситуацій і екстреного реагування (ООН-СПАЙДЕР);
- Міжнародна робоча група з картування у надзвичайних ситуаціях з використанням супутників та інші.

Водночас, доволі широка підтримка здійснюється Міжнародним союзом електрозв’язку. В рамках МСЕ прийнято низку резолюцій, що визначають і деталізують діяльність в сфері електрозв’язку та інформаційно-комунікаційних технологій в цілях контролю і управління у надзвичайних ситуаціях і на випадок лиха. А саме:

– Резолюція № 36 (Анталія, 2006 р.) Повноважної конференції про електрозв’язок і інформаційно-комунікаційні технології на службі гуманітарної допомоги;

– Резолюція № 136 (Анталія, 2006 р.) Повноважної конференції про використання електрозв’язку і інформаційно-комунікаційних технологій в цілях контролю і управління в надзвичайних ситуаціях і у випадках лиха для їх раннього попередження, запобігання, пом’якшення їх наслідків і надання допомоги;

– Резолюція № 34 (Доха, 2006 р.) Всесвітньої конференції з розвитку електрозв’язку (ВКРЕ) про роль електрозв’язку і інформаційно-комунікаційних технологій при ранньому попередженні та пом’якшенні наслідків лиха та при наданні гуманітарної допомоги, а також Питання 22/2 МСЕ-D “Використання ІКТ в області управління операціями на випадок лиха, ресурсів і активних і пасивних систем зондування космічного базування стосовно до надання допомоги на випадок лиха і надзвичайних ситуацій”;

– Резолюція № 48 (Доха, 2006 р.) ВКРЕ про зміцнення співробітництва регуляторних органів в області електрозв’язку;

– Резолюція № 644 (перегл. ВКРЕ-07) про використання ресурсів радіозв’язку для раннього попередження, пом’якшення наслідків лиха і для операцій з надання допомоги при лихах;

– Резолюція № 647 (ВКРЕ-07; 2007 р.) Керівні вказівки по управлінню використанням спектру для радіозв’язку в надзвичайних ситуаціях і для надання допомоги при лихах та інші.

Таким чином, в розвиток положень Конвенції Тампере, складається доволі широкий спектр міжнародних актів, що конкретизують її положення.

Висновки.

У загальному контексті надання гуманітарної допомоги у випадку надзвичайних ситуацій і стихійних лих, *Конвенція про надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій із надання допомоги 1998 року* визначає і забезпечує:

(a) міжнародно-правову основу для розгортання і використання електрозв’язку при наданні міжнародної гуманітарної допомоги,

(b) міжнародно-правову основу гарантованого оперативного надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій з надання допомоги,

(c) міжнародно-правову основу (своєчасного, оперативного, повного та достовірного) отримання, обміну і поширення інформації про небезпечні природні явища, небезпеку для здоров’я людей і лиха, а також

(d) сприяє міжнародному співробітництву в області зменшення масштабів впливу стихійних лих.

Разом з тим, положення Конвенції, враховуючи двадцятирічний досвід її використання набувають:

(e) конкретизації через регулярну діяльність Всесвітніх конференцій ООН,

(f) практичної реалізації через діяльність міжнародних універсальних організацій та їх міжнародних програм, платформ, робочих груп,

(g) деталізації через діяльність з міжнародно-правового регулювання в сфері електрозв’язку та інформаційно-комунікаційних технологій в цілях контролю і управління у надзвичайних ситуаціях і на випадок лиха.

Використана література

1. Про надання телекомунікаційних ресурсів для пом’якшення наслідків лих і здійснення операцій із надання допомоги : Конвенція ООН (Тампере) від 18 червня 1998 року. – Режим доступу : http://www.un.org/ru/documents/decl_conv/conventions/tampere.shtml

2. Сивко Л.Р. Міжнародно-правова регламентація відносин пов’язаних із діяльністю на випадок стихійних лих : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.11 / Київський національний університет імені Тараса Шевченка. – К., 2010. – 29 с.

3. Status Tampere Convention on the Provision of Telecommunication Resources for Disaster Mitigation and Relief Operations 1998. – Режим доступу : https://treaties.un.org/ Pages/ViewDetails. aspx?src=TREATY&mtdsg_no=XXV-4&chapter=25&lang=en&clang=_en

4. Международное сотрудничество в области гуманитарной помощи в случае стихийных бедствий – от чрезвычайной помощи к развитию : Резолюция 69/243 ГА ООН от 23 декабря 2014 года. – Режим доступу : http://www.un-spider.org/sites/default/files/ARES69243_R.pdf

5. Статут Міжнародного союзу електрозв’язку 1992 року. – Режим доступу : http://zakon4. rada.gov.ua/laws/show/995_099

6. Комиссия международного права : Второй доклад о защите людей в случае бедствий, подготовлен Специальным докладчиком Эдуардо Валенсией Оспиной от 7 мая 2009 года. – Режим доступу : http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=4a5aefda2

7. Укрепление координации в области чрезвычайной гуманитарной помощи Организации Объединенных Наций : Резолюция 51/194 ГА ООН от 10 февраля 1997 года. – Режим доступу : https://documents-dds-ny.un.org/doc/UNDOC/GEN/N97/766/29/PDF/ N9776629. pdf?OpenElement

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

УДК 342.951:351.82

ЧОРНОУС А.Г., аспірант кафедри адміністративного права юридичного факультету, Київський національний університет імені Тараса Шевченка

ІНФОРМАЦІЙНІ РЕСУРСИ ЯК ЕЛЕМЕНТ НАЦІОНАЛЬНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ: ЇХ СТВОРЕННЯ ТА ВИКОРИСТАННЯ

Анотація. *У статті розглянуто доктринальні та правові підходи до визначення інформаційних ресурсів як основоположного елементу Національної інформаційної інфраструктури України. Досліджено зарубіжні та національний підходи до детермінування вказаної категорії, а також досліджено ґенезу та поточний стан правової регламентації інформаційних ресурсів в Україні.*

Ключові слова: *інформаційна інфраструктура, інформаційні ресурси, фактори впливу, об’єкти інфраструктури, суб’єкти відповідальності, чинники інформаційної інфраструктури.*

Summary. *The articles considers doctrinal and legal approaches to the definition of information resources as the fundamental element of the National Information Infrastructure of Ukraine. The author examines foreign and national approaches to the determination of information resources, their genesis and current legal regulation status in Ukraine.*

Keywords: *information infrastructure, critical information infrastructure, factors of influence, infrastructure objects, subjects of responsibility, and factors of information infrastructure.*

Аннотация. *В статье рассмотрены доктринальные и правовые подходы к определению информационных ресурсов как основополагающего элемента Национальной информационной инфраструктуры Украины. Исследованы зарубежные и национальный подходы к детерминированию указанной категории, а также исследованы генезис и текущее состояние правовой регламентации информационных ресурсов в Украине.*

Ключевые слова: *информационная инфраструктура, критическая информационная инфраструктура, факторы влияния, объекты инфраструктуры, субъекты ответственности, факторы информационной инфраструктуры.*

Постановка проблеми. Всупереч позитивній динаміці розвитку електронних інформаційних ресурсів в Україні, невирішеними хронічними проблемами діяльності органів публічної адміністрації залишаються відомчий підхід до їх створення, постійне дублювання інформації, відсутність єдиних стандартів, несумісність окремих інформаційних ресурсів, складність пошуку та доступу до окремих видів інформації тощо. Очевидно, що подібні проблемні питання на лише погіршують умови надання та отримання адміністративних послуг за допомогою інформаційно-комунікаційних технологій, а також негативно впливають на бізнес-процеси в Україні та за її межами.

Сучасна організація роботи державних інформаційно-аналітичних систем органів публічної адміністрації характеризується своєю неузгодженістю та децентралізацією. У зв’язку з відсутністю єдиних стандартизованих форматів даних, класифікаторів баз даних, узгоджених протоколів обміну та довідників функціональні можливості працівників органів державної влади та органів місцевого самоврядування суттєво обмежуються в ході їх професійної діяльності.

Існуюча панорама концепцій інформаційного суспільства переконує в необхідності реагування на зміну парадигми суспільного розвитку, в тому числі з боку державних

інститутів. При цьому вказані проблеми мають комплексний міжвідомчий характер та існують на різних рівнях влади, отже не можуть бути вирішені без централізованих та скоординованих організаційно-технологічних заходів та рішень [14, с. 138].

Перехід до інформаційного суспільства має здійснюватися при активній ролі держави, яка бере на себе організацію інформаційно-комунікаційної системи в публічній сфері. Саме держава розробляє цілісну політичну концепцію переходу до інформаційного суспільства, вказує на необхідні для цього програми та стратегії, а також забезпечує наявність загальних умов для розвитку інформаційно-комунікаційних технологій [3]. Окрім цього, серед найбільш типових проблем формування та використання інформаційних ресурсів доцільно виділити галузевий принцип інформатизації державних органів, не орієнтованість державних органів на задоволення потреб населення та неузгодженість і несумісність форматів даних, які зберігаються в публічних інформаційних системах.

Формування ефективної системи управління національними інформаційними ресурсами України є стратегічним напрямком державної політики і потребує від органів державної влади вирішення багатьох проблем, що виникають на даному етапі розвитку національного інформаційного суспільства.

Відтак, з метою активізації ролі держави при побудові ефективно функціонуючої інформаційно-комунікаційної системи Національної інформаційної інфраструктури України та розв’язання інших вище описаних проблем необхідним є створення належного теоретико-правового підґрунтя для подальшої правової регламентації інформаційних ресурсів в Україні. Окрім цього, серед проблемних питань, пов’язаних з формуванням та використанням інформаційних ресурсів, варто виділити:

а) переважно галузевий принцип інформатизації державних органів, що призводить до формування електронних інформаційних ресурсів, орієнтованих, як правило, на задоволення потреб обмеженого кола користувачів;

б) відсутність у державних органах та організаціях орієнтації на інформаційне обслуговування громадян;

в) неузгодженість і несумісність форматів даних, які зберігаються в різних інформаційних системах, несумісність регламентів і технологій їхнього відновлення, використання різних систем класифікацій і лінгвістичних засобів, що призводить до неоднозначності й суперечливості інформаційних ресурсів різних відомств, неможливості їхнього спільного використання і міжгалузевої взаємодії (non-interoperability);

г) відсутність сталої системи зберігання та архівування державних електронних документів, документів електронної пошти та електронних копій паперових документів, а також прийнятих на державному рівні технологій довготривалого зберігання електронних інформаційних ресурсів;

д) відсутність єдиних правових норм, які регулюють доступ до національних інформаційних ресурсів, регламентують порядок передачі та використання інформації про діяльність органів державної влади, підприємств і організацій у відкритих мережах і відповідають вимогам інформаційної безпеки.

Ці та інші проблеми в області формування і використання національних інформаційних ресурсів, аналіз їхніх причин свідчать про необхідність корінної зміни пріоритетів у державній політиці в цьому напрямку та законодавчого усунення існуючих прогалин.

Метою статті є системний аналіз та узагальнення існуючих доктринальних та нормативних (національних та міжнародних) підходів до визначення поняття “інформаційний ресурс” як основоположного елементу національної інформаційної

інфраструктури України; створення необхідного теоретико-правового підґрунтя для подальшого законодавчого закріплення поняття “інформаційний ресурс” на законодавчому рівні.

Виклад основного матеріалу. В контексті сучасних глобалізаційних процесів значення матеріальних, природних, трудових, енергетичних та інших ресурсів зменшується у порівнянні з інформаційними ресурсами, які, хоча й існували раніше, почали здобувати економічно-вартісну оцінку доволі нещодавно.

Інформаційні ресурси виступають основою знання, яка здатна акумулювати в собі досвід людства і визначати подальший вектор його розвитку. За допомогою інформаційних ресурсів індивідуальні знання перетворюються на колективні, що дозволяє вважати інформаційні ресурси основою держави та, зокрема, її владно-управлінської діяльності. Створювані на основі інформаційних ресурсів інформаційні продукти і послуги стали одним з основних товарів на сучасному ринку. Обсяг і якість інформаційних ресурсів, їх раціональне використання здатне покращити економічні показники країни не менше, ніж наявність у неї родовищ нафти або газу.

Щодо поняття та визначальних особливостей інформаційного ресурсу, то в структурному та предметному сприйнятті інформаційний ресурс являє собою окремий документ, сукупність документів або інший візуально об’єкт, який акумулює відомості (інформацію), сформовану за певною ознакою або критерієм [4, с. 130].

Інформаційні ресурси можуть бути представлені різними масивами інформації, які створюються на основі діяльності органів державної влади, на основі діяльності їх відомств, орієнтованих на реалізацію певних владно-управлінських функції. На основі інформації, що формується цими органами і надходить до них внаслідок функціональної взаємодії з іншими суб’єктами, створюються тематичні інформаційні ресурси. Вони можуть бути централізованими або територіально розподіленими. Такі ресурси обов’язково пов’язані між собою і утворюють єдину мережу відомчого або регіонального характеру. Окрім цього, в своїй структурі вони мають інформаційні ресурси іншого організаційного порядку, які додатково взаємодіють по вертикалі і горизонталі між органами публічної адміністрації та споживачами адміністративних послуг [4, с. 132].

Як відзначає провідний фахівець у сфері інформаційного права Бачило І.Л., інформаційні ресурси є потенціалом і рушійною силою розвитку держави на початку третього тисячоліття [5, с. 5].

Питання визначення місця інформаційних ресурсів в системі ресурсів країни, правове регулювання обігу інформації в інформаційних ресурсах, формування інфраструктури для повноцінного використання інформаційних ресурсів є актуальними на сучасному етапі. Важливими проблемами можна вважати питання організації використання інформаційних ресурсів, збереження культурної та історичної спадщини країни, забезпечення, з одного боку, збереження інформаційних ресурсів, а з іншого боку – їх доступності [8, с. 18].

Нисневич Ю.А. вказує в одній зі своїх робіт, що вирішення задач державної інформаційної політики вимагає формування і розвитку інформаційно-комунікаційної інфраструктури держави. Під такою інфраструктурою він пропонує розуміти комплекс організаційних і технологічних засобів пошуку, зберігання, поширення і використання інформаційної продукції і послуг у всіх сферах життєдіяльності суспільства і держави, включаючи територіально-розподільчих депозитаріїв інформаційних ресурсів, державні та корпоративні комп'ютерні мережі, системи спеціального призначення і загального користування, лінії зв'язку і канали передачі даних, засоби комутації та управління інформаційними потоками, організаційні структури управління і контролю [9, с. 2].

В той же час, на думку Пархоменка В.Д., найбільш прийнятним термінологічним визначенням інформаційного ресурсу є таке, відповідно до якого інформаційні ресурси – це окремі документи і масиви документів, результати інтелектуальної, творчої та інформаційної діяльності, бази та банки даних, всі види архівів, бібліотеки, музейні фонди та інші, що містять відомості і знання, зафіксовані на відповідних носіях інформації, є об’єктами права власності всіх суб’єктів України і мають споживчу вартість (політичну, економічну, соціокультурну, оборонну, історичну, ринкову, інформаційну тощо) [11, с. 31].

Необхідність класифікації інформаційних ресурсів досить часто згадувалася в юридичній літературі. Найбільш поширений розподіл інформаційних ресурсів на державні (що формуються державною владою або за рахунок держави) і недержавні (формуються за рахунок приватного сектора економіки) [2, с. 10].

Нисневич Ю.А., у свою чергу, визначив всю сукупність інформаційних ресурсів як національні інформаційні ресурси. Національні інформаційні ресурси повинні утворювати єдину, взаємопов’язану систему, яка виключає виникнення “інформаційного хаосу”, викликаного прагненням до інформаційного суверенітету, породжує надмірний дублювання інформації. Він вказує і на необхідність забезпечити вільний доступ до таких ресурсів і взаємний обмін інформацією. Для досягнення названих цілей, зокрема, взаємодії ресурсів, істотне значення має сумісність документів, інформаційних продуктів, комунікативних систем. Проблема сумісності, як зазначено вище, повинна вирішуватися через стандартизацію результатів інформаційної діяльності: документів, інформаційних ресурсів.

Інформаційний ресурс набуває особливих властивостей, сутність яких і робить його інформаційним продуктом для споживання. Для того, щоб стати інформаційним ресурсом, потоки інформації повинні мати деякі специфічні характеристики, завдяки яким вони стають соціально значущими, технологічно придатними, тобто такими, що мають цінність для практичного застосування. Основною такою характеристикою є системна організація інформаційних потоків та їх окремих елементів. Сучасними формами організації інформаційного ресурсу є: файл, база даних, банк даних, база знань, бібліотека, центр паперово-технічної інформації та ін. Сьогодні, за умов підвищеного динамізму суспільних процесів (швидка зміна ситуації, невизначеність, непередбачуваність і суперечливість як самих соціальних дій, так і їхніх наслідків) конче необхідна розробка повноцінної теоретичної концепції, методології й конструктивної теорії інформаційних ресурсів [7, с. 64].

Враховуючи важливість інформаційних ресурсів, що створюються органами державної влади в порядку здійснення основної діяльності цих органів, такі ресурси в обов’язковому порядку відносяться до національних інформаційних ресурсів [15, с. 46].

Так, на думку Аблякімова Е.Е., державні електронні інформаційні ресурси – це впорядковані масиви даних та електронних документів в інформаційно-телекомунікаційних системах, держателями або розпорядниками яких є органи державної влади або державні підприємства, установи та організації [1, с. 18].

Як слушно зазначає Городов О.О., через інформаційні ресурси опосередковується провідна форма організаційного вираження документованої інформації, яка використовується під час її збирання, обробки, зберігання та споживання [6, с. 113], тобто під час інформаційної діяльності.

Одне з історично перших офіційних тлумачень поняття інформаційного ресурсу міститься в Законі України “Про науково-технічну інформацію” від 25 червня 1993 року № 3322-XII [12], в якому інформаційний ресурс визначається як “сукупність довідково-

інформаційних фондів з необхідним довідково-пошуковим апаратом і відповідними технічними засобами зберігання, обробки і передачі, що є у володінні, розпорядженні, користуванні державних органів і служб науково-технічної інформації, наукових і науково-технічних бібліотек, комерційних центрів, підприємств, установ і організацій”.

Таким чином, відповідно до вказаного підходу, інформаційний ресурс складається з двох взаємопов’язаних елементів: інформації (тобто сукупності довідково-інформаційних фондів) та певної інформаційної системи, що забезпечує користування цим ресурсом (довідково-пошуковий апарат і технічні засоби зберігання, обробки та передачі даних).

На законодавчому рівні дане визначення міститься в Законі України “Про Національну програму інформатизації” від 04 лютого 1998 року № 74/98-ВР [13], де останній визначається як сукупність документів у інформаційних системах (бібліотеках, архівах, банках даних тощо). Аналогічне визначення міститься у Наказі Державного комітету зв’язку та інформатизації України “Про затвердження Методики визначення належності бюджетних програм до сфери інформатизації” від 06 червня 2003 року № 512/7833.

Доволі схоже визначення інформаційного ресурса міститься у Федеральному Законі Російської Федерації “Про інформацію, інформатизації і захисту інформації” від 20 лютого 1995 року № 24-ФЗ [10], в якому інформаційні ресурси визначені як “окремі документи та окремі масиви документів, документи і масиви документів в інформаційних системах (бібліотеках, архівах, фондах, банках даних, інших інформаційних системах)”.

Законом “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” передбачалося, що серед основних напрямів розвитку інформаційного суспільства в Україні слід визначити створення загальнодоступних електронних інформаційних ресурсів на основі врахування національних, світоглядних, політичних, економічних, культурних та інших аспектів розвитку України. При цьому при створенні загальнодоступних електронних інформаційних ресурсів слід забезпечити генерування національних інформаційних ресурсів в економічній, науково-технічній, соціальній, національно-культурній сферах, охороні довкілля тощо, відповідність електронних інформаційних ресурсів стандартам і технічним регламентам, загальнодержавним, галузевим і локальним класифікаторам і довідникам; створення системи центрів даних, що надають послуги з їхнього зберігання та захисту, збереження в електронному вигляді рідкісних даних, що зберігаються на носіях, які можуть зіпсуватися чи зруйнуватися, із визначенням умов їхнього збереження.

Побічно Доктрина інформаційної безпеки визначає, що серед принципів, за якими має здійснюватися забезпечення інформаційної безпеки України, повинна бути пріоритетність національної інформаційної продукції, а одним з напрямів державної політики у сфері інформаційної безпеки України є розбудова та інноваційне оновлення національних інформаційних ресурсів. При цьому держава з метою забезпечення інформаційної безпеки України має вживати в економічній сфері таких заходів як формування вітчизняної індустрії інформаційних послуг, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів.

Виникнення поняття інформаційних ресурсів безпосередньо пов’язано із зростаючою залежністю від рівня розвитку та ефективності використання засобів обробки та передачі інформації. При цьому інформаційний ресурс виступає як компонент інформаційної інфраструктури, що поєднує в собі дані, засіб їх зберігання, взаємозв’язок між інформаційними елементами, відомості про процеси надходження, зберігання та обробки інформації тощо. Таким чином, під інформаційними ресурсами розуміється документована інформація, що зберігається в різних інформаційних

системах (комп’ютерних базах і банках даних, бібліотеках, архівах, інформаційних сховищах тощо).

При цьому під документованою розуміється інформація, зафіксована на матеріальному носії з реквізитами, що дозволяють її ідентифікувати (тобто друкована, теле- і радіопродукція державних та інших засобів масової інформації не є предметом даного дослідження). З розвитком технологій на передній план стали висуватися проблеми власності і володіння інформаційних ресурсів, визначення прав доступу, формулювання вимог до інформаційного ресурсу як товару. Певні інформаційні ресурси в державі стали набувати статусу національних. Це, в першу чергу, інформаційні ресурси, які містять інформацію з різноманітних аспектів діяльності органів державної влади і місцевого самоврядування, а також юридичних осіб і громадян, що відповідають визначеним вимогам до структури й утримання, та зареєстровані відповідно до регламентованої процедури. Наприклад, найбільш розвинутою в країні є сфера національних ресурсів науково-технічної інформації. Крім того, для України на даному етапі її розвитку, формування системи управління національними інформаційними ресурсами є стратегічним напрямком і потребує від органів державної влади вирішення проблем, що виникають, з єдиних методологічних позицій [1, с. 18].

Таким чином, серед комплексу заходів, що, згідно з наведеними державними актами, мають забезпечити розвиток національних інформаційних ресурсів, варто виділити подальше удосконалення нормативно-правової та методологічної бази формування, обліку, використання і захисту інформаційних ресурсів, розвиток інфраструктури інформаційних ресурсів та формування самостійної системи інформаційних ресурсів органів державної влади як вагомої складової сучасної національної інформаційної інфраструктури.

Висновки.

Серед найбільш типових проблем, що виникають в ході формування та використання інформаційних ресурсів, варто виділити галузевий принцип інформатизації державних органів, не орієнтованість органів державної влади на задоволення потреб населення, неузгодженість і несумісність форматів даних, які зберігаються в публічних інформаційних системах, відсутність сталої системи зберігання та архівування електронних баз даних органів публічної адміністрації, а також відсутність єдиної нормативно-правової регламентації отримання доступу до інформаційних ресурсів публічної адміністрації.

З метою усунення вказаних типових проблем необхідним є нормативне (законодавче) визначення поняття “інформаційний ресурс” як основоположного елементу національної інформаційної інфраструктури України.

Узагальнивши та проаналізувавши існуючі доктринальні та нормативні визначення поняття інформаційного ресурсу останній варто визначити як документ або масив документів в інформаційних системах (бібліотеках, архівах, банках даних та інших інформаційних системах). Залежно від організаційної належності інформаційні ресурси підлягають поділу на національні (державний рівень) та глобальні (міжнародно-правовий вимір).

Використана література

1. Аблякімов Е.Е. Правові основи формування державних електронних інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня к.ю.н. : спец. 12.00.07 / Е.Е. Аблякімов. – К., 2010. – 18 с.

2. Антопольский А.Б. Проблемы классификации информационных ресурсов // Научно-техническая информация. – (Сер. 1. Организация и методика информационной работы). – 1997. – № 8. – С. 10-11.

3. Архипова Є.О. Електронне урядування як форма організації державного управління // Державне управління : удосконалення та розвиток. – 2015. – № 4. – (Електронне наукове фахове видання). – Режим доступу : http://www.dy.nayka.com.ua/?op=1&z=855

4. Бачило И.Л. Информационное право : учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов ; под ред. Б.Н. Топорнина. – [2-е изд., с изм. и доп.]. – СПб. : Юрид. центр Пресс, 2001. – 789 с.

5. Бачило И.Л. Информационные ресурсы развития Российской Федерации : правовые проблемы ; отв. ред. И.Л. Бачило. – М. : Наука, 2003. – С. 5.

6. Городов О.А. Основы информационного права России : учеб. пособие / О.А. Городов. – СПб. : Юрид. центр Пресс, 2003. – С. 113.

7. Загальне документознавство : навч. посібник для студ. вищих навч. закл. / Ю.І. Палеха, Н.О. Леміш. – К. : Ліра-К., 2008. – 395 с.

8. Кривоухов А.А. Правовое регулирование защиты государственных информационных ресурсов : дис. на соискание науч. степени к.ю.н. : спец. 05.13.19 / А.А. Кривоухов. – Воронеж. – 2006. – 224 с

9. Нисневич Ю.А. Системный подход в государственной информационной политике // Научно-техническая информация. – (Сер. 1. Организация и методика информационной работы). – 2000. – № 5. – С. 1-7.

10. Об информации, информационных технологиях и о защите информации : Федеральный Закон Российской Федерации от 27.07.06 г. № 149-ФЗ / “Российская газета”, 2006. – № 165.

11. Пархоменко В.Д. Наукові і організаційні проблеми управління інформаційними ресурсами // Науково-технічна інформація. – 2007. – № 3. – С. 31-36.

12. Про науково-технічну інформацію : Закон України від 25.06.93 р. № 3322-XII // Відомості Верховної Ради України (ВВР). – 1993. – № 33. – Ст. 345.

13. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України (ВВР). – 1998. – № 27. – Ст. 181.

14. Талапина Э.В. Модернизация государственного управления в информационном обществе: информационно-правовое исследование : дис. на соискание науч. степени д.ю.н. : 12.00.13 / Э.В. Талапина. – М. – 2015. – 469 с.

15. Основи інформаційного права України : навч. посіб. / [В.Д. Гавловський, В.С. Цимбалюк та ін.] ; за ред. М.Я. Швеця, Р.А. Калюжного, П.В. Мельника. – [2-е вид., перероб. і допов.]. – К. : Знання, 2009. – 414 с.

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

Правова інформатика

УДК 002.55:002.6+342.951

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

РОЗВИТОК ЕЛЕКТРОННОГО ПАРЛАМЕНТАРИЗМУ ЯК ОЗНАКА ПОДАЛЬШОЇ ДЕМОКРАТИЗАЦІЇ ДЕРЖАВИ

Анотація. *В статті досліджуються питання впровадження та розвитку електронного парламентаризму, як ознаки розвитку електронної демократії в державі та руху до побудови в країні інформаційного суспільства; розкриваються напрями та шляхи розбудови електронного парламенту, його складових, а також очікувані результати від його впровадження.*

Ключові слова: *веб-сайт, е-демократія, е-парламентаризм, е-парламент, інформаційно-комунікаційні технології, комунікації.*

Summary. *The article explores the questions of introduction and development of electronic parliamentarism, as a sign of the development of e-democracy in the state and the movement towards building an information society in the country; the directions and ways of development of the electronic parliament, its components, as well as the expected results from its implementation are revealed.*

Keywords: *web-site, e-democracy, e-parliamentarism, e-parliament, information and communication technologies, communications.*

Аннотация. *В статье исследуются вопросы внедрения и развития электронного парламентаризма, как признака развития электронной демократии в государстве и движения к построению в стране информационного общества; раскрываются направления и пути развития электронного парламента, его составляющих, а также ожидаемые результаты от его внедрения.*

Ключевые слова: *веб-сайт, е-демократия, е-парламентаризм, е-парламент, информационно-коммуникационные технологии, коммуникации.*

Постановка проблеми. У сучасних умовах державного управління будь-якої країни світу використання інформаційно-комунікаційних технологій (далі – ІКТ) є об’єктивною необхідністю, оскільки завдяки цьому забезпечується більша презентабельність, прозорість, доступність, звітність та ефективність виконання державним органом своїх функцій, і насамперед парламентом. При цьому способи, до яких вдасться парламент для втілення ІКТ у своєму середовищі, вплинуть на характер інформаційного суспільства у відповідній країні, а також на їхній внесок у створення такого суспільства.

Нині в Україні здійснюється розбудова сучасного демократичного суспільства, реалізація його прагнення інтегруватись у Європейський Союз. Однак ці прагнення стикаються з багатьма перепонами, серед яких наслідки світової економічної кризи, внутрішньополітична нестабільність, високий рівень інфляції, корупції та безробіття, зниження довіри громадян до влади тощо. Це свідчить про суттєве зниження ефективності діяльності системи органів державного урядування та органів місцевого самоврядування, необхідність її якісного оновлення шляхом запровадження нових форм і методів управління та сучасного інструментарію на основі ІКТ, одним з яких є впровадження системи електронного урядування.

Електронне урядування розглядається як частина електронної демократії, складовими якої є електронний парламент, електронне законодавство, електронний суд, електронне посередництво, електронні вибори, електронний референдум, електронне голосування, електронні петиції, електронні кампанії, електронні опитування тощо. “Електронний парламент” – законодавчий орган, який набуває більшої ефективності, прозорості, доступності та звітності завдяки ІКТ. Парламент, як центральна демократична установа, як вища представницька установа, відіграє ключову роль у встановленні соціальних та політичних цінностей, які є корисними для всіх членів суспільства, незважаючи на їх різноманітність. Тому для реформування країни та проведення швидких, радикальних та стратегічних реформ парламент має почати із себе.

Ефективна робота Верховної Ради є передумовою успішного реформування країни, а запорукою її ефективної роботи є запровадження електронного парламентаризму. За допомогою вітчизняних та зарубіжних експертів, було вивчено і представлено міжнародний досвід, який може бути використаний для розбудови е-парламентаризму в Україні, а вироблені ними рекомендації успішно застосовуватимуться в розробці насамперед електронного парламенту. Тому започаткування з 2016 року в Україні побудови електронного парламенту, а в 2018 році затвердження Стратегії електронного парламентаризму на 2018 – 2020 роки – практичний крок щодо розбудови електронної демократії в Україні. Як буде реалізовуватися зазначена Стратегія, ефективно чи ні, залежить в першу чергу від фінансування заходів щодо її реалізації, а також від політичної волі осіб, відповідальних за її впровадження.

Метою статті є здійснення аналізу сучасного стану е-парламентаризму в Україні, вивчення запроваджених механізмів та ефективності подальшої розбудови українського е-парламентаризму, виявлення можливих викликів запровадженню Стратегії електронного парламентаризму, а також напрацювання бачення напрямів побудови ефективного е-парламентаризму.

Виклад основного матеріалу. Сучасне постіндустріальне інформаційне суспільство відрізняється від індустріального суспільства тим, що його базовим принципом є надання вільного доступу до інформації та знань на основі широкого використання сучасних ІКТ. Зазначене знайшло своє відображення у проголошеній Генеральною Асамблеєю Організації Об’єднаних Націй Декларації принципів та Плані дій Всесвітнього саміту з питань інформаційного суспільства у Женеві [1], який був проведений у два етапи – в Женеві 10 – 12 грудня 2003 року і в Тунісі 16 – 18 листопада 2005 року. Зазначене стало значною подією як для Організації Об’єднаних Націй, органи якої відіграли провідну керівну роль в організації саміту, так і для всіх зацікавлених у побудові інформаційного суспільства сторін. Після того, як в 1998 році на Повноважній конференції Міжнародного союзу електрозв’язку було запропоновано провести Саміт, підготовка його Женевського і Туніського етапів тривала сім років. Проте, вплив підсумкових документів ВСІС на формування інформаційного суспільства в усіх країнах світу триватиме значно довше. У підсумкових документах Саміту визначені цілі, завдання, контрольні показники, а також напрями дій для розвитку інформаційного суспільства, у якому кожний може створювати інформацію і знання, мати до них доступ, користуватися й обмінюватися ними, що дасть можливість окремим особам, громадам і народам повною мірою реалізувати свій потенціал, сприятиме сталому розвиткові і підвищить якість життя.

Україна активно долучилася до глобального процесу формування відкритого для всіх інформаційного суспільства, в якому кожний буде мати можливість вільно висловити свою думку і бути почутим. 21 вересня 2005 року були проведені парламентські слухання з питань розвитку інформаційного суспільства в Україні. Ці

слухання викликале велику зацікавлення громадськості, наукових і освітянських установ, органів державної влади та органів місцевого самоврядування, а також відповідних міжнародних організацій, предметом діяльності яких є розбудова інформаційного суспільства.

Враховуючи світовий і вітчизняний досвід з розбудови інформаційного суспільства і визнаючи необхідність його подальшого розвитку в Україні з метою підвищення конкурентоспроможності країни, якості життя населення, результативності науки, якості освіти і охорони здоров’я, а також забезпечення створення нових робочих місць та надання можливостей для реалізації здібностей кожною людиною, учасники парламентських слухань запропонували визнати розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування одним із пріоритетних напрямів державної політики. В контексті зазначеного Верховній Раді України запропоновано забезпечити першочерговий розгляд відповідних законодавчих ініціатив з метою створення цілісної законодавчої системи з питань розвитку інформаційного суспільства, а також ініціювати заходи із створення єдиного парламентського інформаційного простору для забезпечення ефективного міжпарламентського співробітництва.

Зазначені та інші пропозиції та рекомендації були схвалені і формалізовані Постановою Верховної Ради України [2]. Впровадження в Україні рішень Всесвітнього саміту і наступна діяльність сприяють досягненню погоджених на міжнародному рівні цілей розвитку, в тому числі Цілей розвитку, проголошених в Декларації тисячоліття. Подолати цифровий розрив, що поки існує всередині країни, є можливим лише за спільної участі державних органів, приватного сектора, громадських організацій та академічної і технічної спільнот. Саме таке інформаційне суспільство, орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток, є метою процесів у сфері ІКТ в Україні.

В контексті зазначеного Верховною Радою України була прийнята Програма інформатизації законотворчого процесу на 2012 – 2017 роки, а також план заходів щодо реалізації Програми [3]. Згідно з рекомендаціями Міжпарламентського Союзу, членом якого є Україна, застосування ІКТ у роботі національних парламентів має відбуватися відповідно до розробленої ними концепції для:

– забезпечення ефективної роботи парламенту, її прозорості та відкритості;

– гарантування безпеки інформаційних ресурсів парламенту і конфіденційності інформації про особу;

– налагодження діалогу між парламентом, народними депутатами України та громадянами;

– поліпшення механізмів звітності парламенту, народних депутатів України перед виборцями;

– забезпечення повного доступу громадян до інформації про роботу парламенту;

– участі у глобальному інформаційному суспільстві.

Нагальність розроблення і виконання Програми зумовлена необхідністю переходу на принципово новий рівень автоматизації технічних процедур, пов’язаних з діяльністю народних депутатів України, формування актуального парламентського електронного інформаційного ресурсу та ретроспективного оцифровування парламентської документації з метою більш ефективного використання наявних інформаційних ресурсів для реалізації повноважень Верховної Ради України.

Пріоритетним завданням Програми передбачалося створення інтегрованої електронної інформаційно-аналітичної системи “електронний парламент” (далі – Система) та її центральних підсистем:

– “електронний офіс народного депутата України”;

– “електронний комітет”;

– “електронна Погоджувальна рада“”;

– “електронна бібліотека та архів”;

– “електронна зала пленарних засідань: система електронного голосування та підрахунку голосів, система стенографування, система ведення аудіо- та відеотрансляцій та архіву пленарних засідань Верховної Ради України”;

– “система електронного документообігу і контролю виконання доручень Верховної Ради України”;

– “система електронного цифрового підпису”;

– “комплексна система захисту інформації в автоматизованих системах Верховної Ради України”.

Створення Системи, у тому числі за визначенням Глобального центру інформаційно-комунікаційних технологій у парламенті при Міжпарламентському Союзі, означає, що законодавчий орган набуде більшої ефективності, прозорості, доступності та звітності.

Так, Система забезпечить не лише повну автоматизацію етапів законотворчого процесу, а й інформаційну взаємодію Верховної Ради України з іншими органами державної влади та органами місцевого самоврядування, громадянами, юридичними особами за допомогою сучасних ІКТ із застосуванням високих стандартів доступу до інформаційних ресурсів парламенту.

Крім того, створення Системи забезпечить сучасні організаційно-інформаційні можливості для реалізації конституційних повноважень Верховної Ради України, сприятиме відкритості у діяльності Верховної Ради України, реалізації конституційних прав громадян, у тому числі в інформаційній сфері.

На думку тодішнього Голови Верховної Ради України В. Гройсмана, створення е-парламенту надасть громадянам: доступні та зрозумілі інтерфейси взаємодії з ВРУ; можливості здійснення он-лайн контролю за роботою ВРУ та депутатів; здійснювати безпосередній вплив на рішення ВРУ через е-петиції, е-звернення, е-обговорення тощо. У свою чергу для законодавців зазначене підвищить ефективність та оперативність їхньої роботи (шляхом впровадження е-кабінету депутата); підвищить їхнє інформаційно-аналітичне забезпечення; забезпечить якісний зворотній зв’язок з громадянами та підвищення їхньої довіри до законодавців.

Передбачалося, що основного економічного ефекту від виконання Програми буде досягнуто завдяки створенню цілісного парламентського документального ресурсу та забезпеченню його використання в установленому чинним законодавством порядку.

Таким чином, використання ІКТ у діяльності представницького органу, яким є парламент, є однією з найбільш перспективних форм електронної демократії. Тобто, електронний парламент як орган законодавчої влади, що як один із центрів концентрації політичної влади спрямований на забезпечення ефективної взаємодії між парламентаріями і представниками громадянського суспільства на засадах верховенства права, прозорості, доступності та підзвітності у своїй діяльності, за рахунок ефективного використання ІКТ.

Оновлення формату взаємовідносин відбувається за наступними напрямами:

– легальний, тобто, у законодавчому процесі – організація документообігу та здійснення ефективної міжнародної діяльності;

– комунікативний – зменшення перешкод для вільного спілкування за рахунок використання соціальних мереж та сайтів;

– технологічний, тобто еволюція технологій, модернізація інформаційних сервісів;

– інтерактивний – покращення інституційно-функціональних параметрів взаємодії, посилення безпосередньої участі, запровадження інтеграції між парламентом і громадянами.

В Україні робота електронного парламенту фактично започаткована в 2015 році відповідно до Програми [3], про що оголосив 3 лютого 2016 року тодішній Голова Верховної Ради України В. Гройсман. Інформаційно-аналітична система включала в себе наступні елементи: електронний офіс народного депутата (стаціонарний і мобільний); електронний комітет; електронну Погоджувальну раду; електронну бібліотеку та архів; електронну залу пленарних засідань; електронний документообіг; контроль виконання доручень Верховної Ради України; систему електронного цифрового підпису; комплексну систему захисту інформації; інтегровану базу даних законотворчого процесу [4].

Основою програмного комплексу “Е-Парламент” стали відповідні автоматизовані системи Верховної Ради України стосовно реалізації процедур законодавчого процесу, автоматизації документообігу, кадрового забезпечення, функціонування інформаційно-пошукових систем та ін., наприклад, комп’ютерна технологія інтегрованої обробки текстів законопроектів для підготовки до розгляду Верховною Радою України (“ЗАКОНОТВОРЕЦЬ”), інформаційно-пошукова система “ЗАКОНОДАВСТВО”, системи відкритого електронного голосування “РАДА”, “Графіт”, інформаційно-пошукова система “Адміністративно-територіальний устрій України”.

Із лютого 2016 р. розпочалося масштабне впровадження електронного парламенту у Верховній Раді України за трьома етапами: технічне переозброєння; навчання народних депутатів та працівників Апарату Верховної Ради; промислова експлуатація. Поставлена мета була узгоджена з європейськими стандартами інформатизації діяльності парламенту та мала дозволити в інтерактивному сервісному режимі налагодити ефективну взаємодію між органом законодавчої влади та громадськістю, у тому числі зі залучення інструментів електронного урядування.

Фундаментом такої оновленої парадигми взаємодії виступали категорії доступності, прозорості, відкритості, гарантування технічного захисту інформації, впровадження дистанційної роботи членів парламенту та забезпечення ефективного громадського контролю за прийняттям рішень Верховною Радою України.

На даному етапі мова йшла про оцифрування документів, модернізацію робочих місць (діловодів, працівників юридичного та науково-експертного управлінь, комітетів), запровадження Wi-Fi та мережевої інфраструктури, оновлення серверних ресурсів, створення модельної зали для засідань комітетів, перехід на безпаперову роботу парламенту (е-комітети, е-порядок денний пленарного засідання, е-протоколи, електронні приймальні), забезпечення функціонування сервісу е-петицій, порталу відкритих даних.

Подальше забезпечення інформатизації діяльності парламенту мало стосуватися інфраструктурних, інформаційно-навчальних, комунікативних тактичних кроків (розробка та імплементація програмних рішень; навчання народних депутатів і працівників Апарату Верховної Ради України щодо роботи в новому інформаційному середовищі; введення новітніх електронних продуктів і сервісів; налагодження результативної співпраці з громадськістю та приватним сектором).

Таким чином, відповідна сукупність веб-порталів, систем, комп’ютерних технологій фактично забезпечувала інфраструктурно-технічні аспекти взаємодії складових елементів цих комплексів та інших інформаційних ресурсів, учасників законодавчого процесу між собою, а також парламенту з публічною адміністрацією, автоматизацію процесів обліку майна та стану фінансових зобов’язань, ведення електронного документообігу й обробки офіційного електронного документу, повноцінне впровадження електронного цифрового підпису, у тому числі з додаванням посиленого сертифіката відкритого ключа, при створенні документів, соціометричні дослідження відносин персоналу, здійснення державних закупівель в електронній формі тощо.

Необхідно зазначити, що реалізація такого масштабного проекту як Програмний комплекс “Е-Парламент” має використовувати хмарну архітектуру. Для цього, у першу чергу, необхідно виконати побудову “парламентського хмарного” Центру Обробки Даних з перспективою на те, що він може стати загальнодержавним центром хмарних обчислень для реалізації програми розвитку електронного уряду. У “хмарі” Верховної Ради України мають бути розміщені всі обчислювальні ресурси (мережі передачі даних, сервери, пристрої зберігання даних, додатки та сервіси), які можуть, за рахунок моделі роботи “хмарних технологій”, оперативно надаватися кінцевим користувачам, розробникам додатків і сервісів, архітекторам ІКТ.

Отже, ключовими характеристиками змін у контексті інформатизації законотворчого процесу Верховної Ради України можна вважати інфраструктурні питання, послуги, визначення способу користування, тренування персоналу, комунікацію між парламентом і членами громадянського суспільства. Основним досягненням у цьому контексті стало започаткування створення такого електронного середовища діяльності парламенту, яке має відповідати уявленням репрезентативності, прозорості, доступності, підзвітності та ефективності за умов полегшення та підвищення координації роботи та співпраці між усіма учасниками відносин у сфері функціонування електронного парламенту. Роль ІКТ в цих процесах стосується встановлення зв’язків між характеристиками е-парламенту та допомога парламенту у виконанні визначених повноважень (більша якість інформації, кращий доступ, ефективна організація роботи тощо) [4].

Таким чином, у питанні впровадження е-парламенту були зроблені перші кроки в якості запровадження та функціонування перелічених вище складових, що, на нашу думку, слугує стартовою позицією для подальшого впровадження е-парламенту у повному обсязі.

Водночас, залишається технічно не вирішеним, а це не відповідає положенням Конституції України (ч. 3 ст. 84), таке ключове для діяльності парламенту питання, як особисте голосування депутатів на засіданні Верховної Ради України. Крім того, введення електронного документообігу у діяльності парламенту відкладалося, і лише на початку 2018 року Головою Верховної Ради України було заявлено про його запровадження [5], і це при тому, що з 2015 року депутати не можуть прийняти законопроект про внесення змін до Регламенту ВРУ (для оптимізації законодавчого процесу) щодо запровадження електронного документообігу [6]. Проектом передбачається надання нардепам, комітетам, тимчасовим спеціальним комісіям, тимчасовим слідчим комісіям, депутатським фракціям (депутатським групам) проекту порядку денного сесії ВРУ, проекту рішення про внесення змін до затвердженого порядку денного сесії ВР, розкладу пленарних засідань сесії Верховної Ради, порядку денного на наступний день пленарних засідань. Так, інформаційні листи про проект порядку денного сесії ВР, проект рішення про внесення змін до затвердженого порядку

денного сесії Ради, розклад пленарних засідань сесії, порядок денний на наступний день пленарних засідань мають надсилатися нардепам, комітетам, тимчасовим спеціальним комісіям, тимчасовим слідчим комісіям, депутатським фракціям (депутатським групам) у день розміщення таких документів на офіційному веб-сайті Верховної Ради. Інформаційний лист має містити посилання на відповідні сторінки офіційного веб-сайту Верховної Ради. Вказаний інформаційний лист, висновки, підготовлені головним комітетом до першого, повторного першого, другого, повторного другого, третього читання законопроектів, висновки інших комітетів та інші супровідні документи до законопроектів, пропозиції щодо усунення неузгодженостей чи редакційних неточностей у прийнятому законі, пропозиції президента України до поверненого ним закону разом з висновком головного комітету, порівняльною таблицею та іншими супровідними документами надсилатиметься депутату на адресу електронної пошти на поштовому сервері ВРУ на початку робочого для, наступного за днем розміщення таких документів у базі даних законопроектів електронної комп’ютерної мережі веб-сайту Верховної Ради України.

При цьому законопроекти, що розглядаються парламентом за спеціальними процедурами, та супровідні документи до них, на всіх стадіях опрацювання і розгляду надаються народним депутатам в паперовому вигляді, а також в електронному – шляхом введення відповідної інформації до бази даних законопроектів електронної комп’ютерної мережі веб-сайту ВРУ. Встановлюється, що з дня надання народним депутатам вказаних документів в електронному вигляді, але не пізніше 15 години п’ятниці, що передує тижню, відведеному для пленарних засідань, народний депутат може подати письмову заяву до Апарату парламенту про надання йому цих документів у паперовому вигляді.

Відкладався також перехід на безпаперову роботу парламенту (е-комітети), хоча і відбулися певні зміни в документообігу: документи, які надходять до Верховної Ради, скануються, і далі вони розглядаються в електронному вигляді. Під час сканування документів одночасно заносяться їхні реквізити і ставиться дата розгляду документів; здійснюється контроль щодо їх виконання; іде процес зміни ідентифікації користувачів, за якого кожен матиме доступ лише до своєї категорії документів; запроваджується система дистанційної роботи з документами; будується система звітності документообігу, яка працюватиме в автоматичному режимі.

Логічним продовженням інформатизації законотворчого процесу, розвитку е-парламенту стало затвердження Стратегії електронного парламентаризму на 2018 – 2020 роки [7]. Зазначене відповідає політиці реалізації Постанови Верховної Ради України від 17 березня 2016 року [8], в якій містяться рекомендації Місії Європейського Парламенту з оцінки потреб, що розроблені з метою підвищення якості українського парламентаризму та викладені у “Доповіді та Дорожній карті щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України”, комплексного вирішення проблем у сфері забезпечення інформаційної та кібернетичної безпеки, і які взяті за основу для реалізації. В Рекомендаціях передбачається забезпечення відкритості, прозорості та підзвітності громадянам законотворчого процесу у Верховній Раді України.

Відповідно до Плану заходів “Відкритий парламент” заплановано забезпечити права громадян України коментувати законопроекти, які зареєстровані у Верховній Раді України та є предметом громадського обговорення (з використанням, зокрема, веб-інтерфейсу та новітніх ІТ-засобів). Крім того, передбачено розробити та схвалити стратегію переходу до електронного парламентаризму, що нині і зроблено, включаючи

середньострокову стратегію Інформаційних та Комунікаційних технологій (на 3 – 5 років). А у співпраці з Адміністрацією Президента України та Кабінетом Міністрів України – розробити стратегію переведення у цифровий формат документообігу, пов’язаного з законодавчим процесом.

Крім того, прийняття Стратегії електронного парламентаризму на 2018 – 2020 роки [7] є своєрідним наступним логічним кроком створення дієвого механізму підвищення довіри до ВРУ, підвищення якості українського парламентаризму, на що, у свою чергу, направлена Комунікаційна стратегія ВРУ на 2017 – 2021 роки [9], і яка була спрямована на підвищення рівня довіри до Верховної Ради України та сприйняття її як ефективної інституції серед громадян України, організацій громадянського суспільства, засобів масової інформації та міжнародних аудиторій. Стратегія [7] передбачає вирішення шести основних завдань:

1) покращення іміджу парламенту шляхом запровадження системних комунікацій за допомогою єдиного комунікаційного центру всередині парламенту, запровадження кодексу етики та правил брендингу Верховної Ради України;

2) підвищення обізнаності громадян щодо парламентських процесів;

3) забезпечення активної участі громадськості у процесі прийняття рішень та налагодження зворотного зв’язку;

4) удосконалення співпраці з парламентськими та незалежними медіа і журналістами, у тому числі міжнародними засобами масової інформації;

5) посилення присутності парламенту на міжнародному рівні;

6) оптимізація внутрішніх комунікацій та обміну інформацією всередині парламенту.

Важливою складовою комунікаційної стратегії є забезпечення зворотного зв’язку з громадянами, громадськими об’єднаннями, засобами масової інформації та міжнародними аудиторіями, а саме: підзвітність громадськості, створення умов для участі в законодавчих процесах та служити надійними вторинними каналами інформування про парламентські процеси.

Відкриваючи церемонію урочистого підписання Стратегії електронного парламентаризму на 2018 – 2020 роки, Голова Верховної Ради України Андрій Парубій наголосив: “Ми робимо Парламент відкритим і прозорим для кожного громадянина. Мені приємно відзначити, що Громадський рух ЧЕСНО, проаналізувавши показники сайтів парламентів 193 країн світу, визнав, що сайт Верховної Ради України, посідає перше місце за кількістю відвідувачів. На парламентський сайт України щомісяця заходить майже 3 млн. відвідувачів, які переглядають сайт понад 7 млн. 800 тис. разів” [10].

Крім того, Голова Верховної Ради України Андрій Парубій зазначив, що з 2019 року у Верховній Раді України будуть введені електронні ідентифікаційні картки для народних депутатів. Завдяки ID-картці народного депутата буде забезпечуватися доступ народного депутата на засідання Верховної Ради України, на засідання комітетів, здійснюватися контроль за персональним голосуванням, яка одночасно також буде і посвідченням для народного депутата. Для цього будуть обладнані комітети і входи в парламент і вже у 2019 році буде планується випробовування цієї системи в тестовому режимі.

Стратегія розроблена на основі аналізу сучасного стану впровадження інструментів електронного парламенту і визначає бачення, місію, мету, цілі, базові принципи подальшого розвитку електронного парламентаризму України. Пріоритетними завданнями Стратегії електронного парламентаризму є автоматизація всіх етапів законотворчого процесу: електронний документообіг, електронний цифровий підпис, персональний кабінет користувача, корпоративний Інтранет-портал для роботи з

електронними документами. Також є необхідність забезпечення електронної взаємодії між Верховною Радою, Кабінетом Міністрів та Адміністрацією Президента України, тобто розроблення стратегії переведення у цифровий формат документообігу, пов’язаного із законодавчим процесом у рамках так званого “законодавчого трикутника”.

Необхідно зазначити, що процесу розроблення Стратегії передувала спільна робота з Генеральним Директоратом з питань інновацій і технологічної підтримки Європейського Парламенту, експертним та громадським середовищем. Згідно з рекомендаціями Міжпарламентського союзу робота сучасних національних парламентів має базуватися на застосуванні ІКТ для забезпечення ефективної роботи парламенту, прозорості, відкритості та підзвітності членів парламенту перед виборцями, налагодження діалогу між парламентом і громадянами, забезпечення повного доступу громадян до інформації про роботу парламенту, участі парламентарів у глобальному інформаційному суспільстві.

З урахуванням системного підходу Стратегія ґрунтується на комплексному впровадженні ІКТ в діяльність Верховної Ради України з урахуванням поточних та майбутніх видів діяльності парламенту, його організаційної та територіальної структури, а також обумовлює, яким чином буде підтримана інституційна складова розвитку Верховної Ради України у форматі електронного парламентаризму. Крім того, враховуються рекомендації Місії Європейського парламенту з оцінки потреб під головуванням Пета Кокса, Президента Європейського парламенту 2002 – 2004 рр., а також міжнародний досвід та останні рейтинги електронного парламентаризму (World e-Parliament Report 2016) Міжпарламентського союзу (Inter-Parliamentary Union).

На сьогодні Погоджувальна рада та два комітети Верховної Ради України активно використовують у своїй роботі зазначені електронні зали засідань, два комітети тестують розроблену автоматизовану систему “Електронне засідання Комітету Верховної Ради України”, що консолідує інформацію про законопроекти з баз даних автоматизованих систем “Документообіг Верховної Ради України” і “Контроль проходження законопроектів” та забезпечує розподіл роботи працівників секретаріатів комітетів над формуванням порядку денного засідань комітетів та підготовкою питань, включених до нього.

Реалізація конституційних повноважень Верховної Ради України та виконання міжнародних зобов’язань, взятих на себе Україною, потребують докорінної зміни як регламентних, так і програмно-технологічних процедур, пов’язаних із основними видами діяльності народних депутатів України в комітетах, фракціях, під час засідань Погоджувальної ради та пленарних засідань, а також роботою у виборчих округах. На сьогодні ж існують певні ризики повного виконання Стратегії:

– офіційний веб-сайт Верховної Ради України містить обмежену кількість публічної інформації, має застарілий інтерфейс, недосконалу англомовну версію й складний пошук інформації;

– бракує “цифрової” стратегії щодо присутності Верховної Ради України у Інтернеті та соціальних медіа;

– низький рівень фінансового забезпечення впровадження ІКТ, відсутність чіткої методології бюджетного прогнозування потреб у сфері ІКТ в бюджетному офісі Верховної Ради України.

Саме недостатній рівень фінансового забезпечення, як показує практика, може тою основною перепоною для успішного виконання згаданої Стратегії, як і Програми інформатизації законотворчого процесу у Верховній Раді України, і Комунікаційної стратегії, так само як і будь-якої стратегії чи програми.

Певним недоліком змісту Стратегії, як сучасного процесуального документу щодо уніфікації функціонування парламенту, на нашу думку є те, що вона не передбачає такий сучасний механізм функціонування парламенту, як офіційне оприлюднення актів Верховної Ради України на її офіційному веб-сайті. В цьому відношенні в позитивному сенсі вирізняються такі органи держави, як Конституційний Суд України та Національний банк України. Так, відповідно до положень частини шостої статті 56 Закону [11], офіційним опублікуванням нормативно-правового акту Національного банку, окрім офіційних друкованих видань, вважається і його перше розміщення на сторінці Офіційного Інтернет-представництва Національного банку України [12]. Подібна новела знайшла своє місце і в статті 94 Закону [13], згідно з якою оприлюднення всіх актів Конституційного Суду за результатами конституційного провадження здійснюється на офіційному веб-сайті Суду.

З огляду на зазначене, а також враховуючи те, що Верховна Рада України є найвищим представницьким органом держави, доцільним було б щоб вона напрацьовувала відповідні рекомендації іншим представницьким органам (органам місцевого самоврядування) щодо механізмів запровадження е-органів місцевого самоврядування, змісту їхніх веб-сайтів, протоколів сумісності з іншими веб-сайтами тощо, так як напрацьовує у своїх актах відповідні рекомендації органам місцевого самоврядування Кабінет Міністрів України. Тим самим закладалися б певні засади створення у майбутньому Національної системи нормативно-правових актів України, що цілковито корелювалося б із запровадженою Концепцією розвитку електронної демократії в Україні [14], згідно з якою до 2020 року має бути створена вся нормативно-правова база для практичного впровадження е-демократії. Концепція містить мету, основні цілі та досягнення, що викладені у 53 комплексних заходах. Під електронною демократією розуміється форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоврядування шляхом широкого застосування ІКТ в демократичних процесах, що дає змогу:

– посилити участь, ініціативність та залучення громадян на загальнодержавному, регіональному та місцевому рівні до публічного життя;

– поліпшити прозорість процесу прийняття рішень, а також підзвітність демократичних інститутів;

– поліпшити зворотну реакцію суб’єктів владних повноважень на звернення громадян;

– сприяти публічним дискусіям та привертати увагу громадян до процесу прийняття рішень. Електронна демократія для простого громадянина – це можливість, не виходячи з дому, впливати на формування та реалізацію державної політики.

Реалізація Концепції [14] передбачена на трьох рівнях – загальнонаціональному, регіональному та місцевому. На національному рівні передбачено створення Фонду розвитку е-демократії, вдосконалення механізму подання та розгляду петицій, масштабне впровадження мережі бюджетів участі тощо. Метою цієї Концепції є формування політичних, організаційних, технологічних та ідеологічних умов розвитку електронної демократії в Україні, що характеризується зростанням широкого долучення громадян до комунікації, співпраці з органами державної влади, контролю за ними, участі у виробленні політики, розвитку самоорганізації та самоврядування, а також рівнем довіри до суб’єктів владних повноважень; узгодження стандартів державної політики зазначеної сфери з міжнародними, зокрема європейськими стандартами. Тим самим очікується підвищення рівня участі, ініціативності та залучення громадян, інститутів громадянського суспільства, суб’єктів господарювання на загальнодержавному, регіональному та місцевому рівні до процесу прийняття управлінських рішень.

Висновки.

На підставі проведеного дослідження можна зробити висновок про те, що розвиток інформаційного суспільства в Україні та впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування визначається одним із пріоритетних напрямів державної політики. Нинішнє суспільство відрізняється від попередніх саме наданням вільного доступу до інформації та знань на основі широкого використання сучасних ІКТ, що знайшло своє відображення у проголошеній Генеральною Асамблеєю Організації Об’єднаних Націй Декларації принципів та Плані дій Всесвітнього саміту з питань інформаційного суспільства.

Наша молода держава долучилася до процесу формування відкритого для всіх інформаційного суспільства, в якому кожний буде мати можливість вільно висловити свою думку і бути почутим. Впровадження новітніх ІКТ в усі сфери суспільного життя і в діяльність органів державної влади та органів місцевого самоврядування є одним із пріоритетних напрямів державної політики. З огляду на зазначене, впровадження в Україні е-урядування, е-парламенту і е-парламентаризму є таким напрямком розвитку е-демократії в країні в цілому.

Важливим кроком у розвитку е-демократії в Україні стала інформатизація законотворчого процесу в цілому та розвиток е-парламенту зокрема, логічним розвитком яких є затвердження Стратегії електронного парламентаризму на 2018 – 2020 роки. Однак успішне впровадження зазначеного значною мірою залежить від наявної політичної волі самої державної влади та належне фінансування нею механізмів впровадження Стратегії. Як показує практика минулих років, саме від дієвості цих складових залежатиме подальше просування українського суспільства у своєму розвитку.

Використана література

1. Підсумкові документи Всесвітнього саміту з питань інформаційного суспільства (Женева 2003 – Туніс 2005). – Режим доступу : http://old.apitu.org.ua/wsis (дата звернення 15.07.2018).

2. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради країни від 01.12.05 р. № 3175-IV. – Режим доступу : http://zakon5.rada.gov.ua/ laws/show/3175-15 (дата звернення 15.07.2018).

3. Про затвердження Програми інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки : Постанова Верховної Ради України від 05.07.12 р. № 5096-VI // Відомості Верховної Ради України (ВВР). – 2013. – № 37. – Ст. 492.

4. В Україні запущено електронний парламент. – Режим доступу : http://pravo.org.ua/ua/news/20871323-v-ukrayini-zapuscheno-elektronniy-parlament (дата звернення 19.07.2018).

5. Рада запровадила електронний документообіг – Парубій. – Режим доступу : https://news.finance.ua/ua/news/-/421904/rada-zaprovadyla-elektronnyj-dokumentoobig-parubij (дата звернення 24.07.2018).

6. Рада планує ввести електронний документообіг у ВРУ. – Режим доступу : https://www.rbc.ua/ukr/news/rada-planiruet-vvesti-elektronnyy-dokumentooborot-1448541017.html (дата звернення 24.07.2018).

7. Про затвердження Стратегії електронного парламентаризму на 2018 – 2020 роки : Розпорядження Голови Верховної Ради України від 05.07.18 р. № 278. – Режим доступу : http://zakon5. rada.gov.ua/laws/show/278/18-рг (дата звернення 24.07.2018).

8. Про заходи з реалізації рекомендацій щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України : Постанова Верховної Ради України від 17.03.16 р. № 1035-VIII // Відомості Верховної Ради України (ВВР). – 2016. – № 14. – Ст. 149.

9. Про додаткові заходи з реалізації Декларації відкритості парламенту : Розпорядження Голови Верховної Ради України від 21.11.17 р. № 486. – Режим доступу : http://zakon0.rada.gov.ua/laws/ file/docs/59/d472407.pdf? noattach=1 (дата звернення 26.07.2018).

10. Голова Верховної Ради України Андрій Парубій: “Ми робимо Парламент відкритим і прозорим для кожного громадянина”. – Режим доступу : http://www.rada.gov.ua/print/160622.html (дата звернення 13.08.2018).

11. Про Національний банк України : Закон України від 20.05.99 р. // Відомості Верховної Ради України (ВВР). – 1999. – № 29. – Ст. 238.

12. Офіційне Інтернет-представництво Національного банку України. – Режим доступу : https://bank.gov.ua/control/uk/publish/category;jsessionid=0AB6B25EC8C598F49A443B1735D0A290?cat_id=8804 895 (дата звернення 13.08.2018).

13. Про Конституційний Суд України : Закон України від 13.07.17 р. // Відомості Верховної Ради України (ВВР). – 2017. – № 35. – Ст. 376.

14. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 08.11.17 р. № 797-р. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/797-2017-p/print1509562034213953 (дата звернення 13.08.2018).

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

УДК 004.44:002.513.5

ЛАНДЕ Д.В., *доктор технічних наук,* керівник наукового центру
НДІ інформатики і права НАПрН України
ЯНЬЦІН ЧЖАО, заступник директора Інституту інформаційних досліджень
Шандуньської академії наук, КНР (ІІД ШАН)
МОЦЗІ ВЕЙ, старший науковий співробітник ІІД ШАН
ШІВЕЙ ЧЖУ, завідувач відділу ІІД ШАН
ЦЗЯНЬПІН ҐО, інженер ІІД ШАН

СИСТЕМА АНОТУВАННЯ КИТАЙСЬКОЇ ПРАВОВОЇ ІНФОРМАЦІЇ

Анотація. *Роботу присвячено методу автоматичного реферування правової інформації КНР, представленої китайською мовою. Розглянуто модель реферату правового документа і принципи його формування. Для вирішення завдання визначення рівня важливості речень з вихідного документа було запропоновано перейти до визначення вагових значень окремих ієрогліфів, а не слів в тексті документів і рефератів.*

Ключові слова: *автоматичне реферування, правова інформація, китайська мова, теорія інформації, мережева модель*

Summary. *Article is devoted to a method of automatic text summarization of the legal information provided in Chinese. The model of the legal document abstract and the procedure of his formation is considered. To determine the level of importance of sentences, it was suggested to proceed to determine the weight values of separate hieroglyphs, rather than words in the text of documents and abstracts. Also consideration of model of documents as networks of sentences for detection of the most important sentences on parameters of this network was offered.*

Keywords: *automatic summarization, legal information, Chinese language, information theory, network model.*

Аннотация. *Работа посвящена методу автоматического реферирования правовой информации КНР, представленной на китайском языке. Рассмотрена модель реферата правового документа и принципы его формирования. Для решения задачи определения уровня важности предложений из исходного документа было предложено перейти к определению весовых значений отдельных иероглифов, а не слов в тексте документов и рефератов.*

Ключевые слова: *автоматическое реферирование, правовая информация, китайский язык, теория информации, сетевая модель*

Постановка проблеми. З постановки завдань штучного перекладу і автоматичного реферування практично починалася комп’ютерна обробка природних мов. Перші фундаментальні роботи з автоматичного реферування текстів з'явилися ще в середині минулого століття [1]. Завдання пов'язане з рішенням найважливішої проблеми – скороченням обсягів інформації, що споживається людиною, боротьби з інформаційним шумом. Це завдання дуже актуальне саме сьогодні через постійне зростання інформаційного простору. Автоматичне реферування відомо всім користувачам мережевих пошукових систем – у відповідь на запит вони отримують не тільки назву документа, але і короткий автоматично створений опис (сніпет), користувачі мобільних пристроїв хочуть бачити короткий опис статей, перш ніж переходять до докладного читання. Особи, які приймають важливі управлінські рішення, повинні ознайомлюватися з тисячами документів на добу, свідомо відкидаючи інформаційний шум.

В даний час існують сотні промислових систем автоматичного реферування, наприклад, такі пакети, як Microsoft Office Word AutoSummarize, Mac OS X Summarize, IBM Tivoli Monitoring Summarization and Pruning Agent, Oracle Text, плагіни для браузерів Chrome, Mozilla.

Відомі численні підходи до автоматичного реферування. Останнім часом, дедалі застосовуються нейромережеві технології, глибинне машинне навчання. Існують також численні лінгвістичні підходи, пов’язані з автоматичним розбором речень, представлених різними мовами. Традиційний тип систем автоматичного реферування – екстрактивний (квазіреферування), при якому реферат складається з окремих, часом слабо пов’язаних між собою речень вихідного документа. Слід зазначити, що сьогодні практично всі промислові системи автоматичного реферування відносяться до екстрактивних систем.

Причин розробки нової системи автоматичного реферування декілька. По-перше, вирішується завдання автоматичного реферування правової інформації. А це тексти, які не можна повною мірою вважати вільними, неструктурованими. Наявна структура окремих видів документів і застосування найкращих універсальних систем реферування не дає задовільних результатів. По-друге, автори мають справу з текстами документів, представленими китайською мовою, що істотно звужує коло можливих для застосування систем. Крім того, для обробки китайських текстів, як правило, необхідна сегментація слів – у китайській мові слова частіше за все не відокремлюються один від одного в тексті. По-третє, має бути розроблена програма, здатна всередині корпоративної системи обробляти великі потоки даних з прийнятною продуктивністю і якістю, вбудована в існуючу систему документообігу.

Крім того, абстрактивний переказ документів в даному випадку неприйнятний. Будь-які “фантазії”, “вольний переказ” комп’ютером правових актів неприпустимі. Вихід виявився один – розробляти деякий гібридний алгоритм і, відповідно, програму екстрактного типу, здатну враховувати особливості правових актів КНР, при цьому програма повинна також бути здатна обробляти окремі документи, які об’єднуються у великі документальні масиви. Ця програма повинна виділяти заздалегідь задані об’єкти в позначених смисловими маркерами частинах документів, виявляти найбільш важливі частини документів (у тому числі і за статистичними критеріями), формувати мережі речень і виводити необхідний обсяг цільової інформації в реферат.

Метою статті є опис нового методу і технології автоматичного реферування правової інформації КНР, представленої китайською мовою.

Виклад основного матеріалу.

Підхід, що пропонується. При вирішенні наведеної проблеми було запропоновано два підходи, які можна вважати новими в даній галузі, а саме, для вирішення завдання визначення рівня важливості окремих речень було запропоновано перейти до визначення вагових значень окремих ієрогліфів, а не слів в тексті документів і рефератів. Також було запропоновано розгляд моделі документів як мережі речень для виявлення найбільш важливих з них за параметрами цієї мережі. Вага зв’язків двох речень у цій мережі визначається нормованою вагою загальних ієрогліфів, що входять в них.

В рамках традиційного статистичного підходу до обробки природних мов вага речень зазвичай обчислюється виходячи з оціночної ваги лексичних одиниць (слів, словосполучень), що входять у ці речення [2 – 5]. В рамках даних робіт пропонується в якості таких елементів для китайської мови використовувати окремі ієрогліфи.

Перехід від розглянутих у класичній моделі слів до ієрогліфів дозволяє уникнути складної процедури сегментування слів у тексті, що неминуче при всіх інших змістовних методах автоматичного аналізу китайських текстів. Звичайно, даний підхід не може бути застосовний до європейських мов, де кількість різних букв не перевищує декількох десятків. Разом з тим для автоматичного реферування китайських текстів запропонований підхід дає прийнятні результати, що буде показано нижче.

Відомо, що в китайській мові існує понад 40 тисяч ієрогліфів, тому кожному з них (нехай окремий ієрогліф не завжди повною мірою відображає смислову одиницю) можна приписати вагове значення, яке розраховується за відомими формулами, наприклад *TF-IDF*, (від англ. *TF* – term frequency, *IDF* – inverse document frequency) [6]. *TF-IDF* – статистична міра, яка використовується для оцінки важливості слова (в даному випадку – не слова, а ієрогліфа) в контексті документа, що є частиною масиву документів. Вага деякого ієрогліфа пропорційна кількості його вживання в документі, і обернено пропорційна частоті появи цього ієрогліфа в усіх документах масиву.

Крім того, на відміну від класичних підходів до визначення вагових значень речень, пропонується нова, мережева модель. В рамках цієї моделі розглядається не спрямована мережа, вузлами якої виступають окремі речення, що входять в документ, між якими встановлюються зв’язки у разі наявності у них загальних ієрогліфів. Вага зв’язку між двома реченнями визначається як сума ваг загальних для цих речень ієрогліфів. На основі цієї мережі розраховується вага кожного речення як сума вагових значень всіх зв’язків, що виходять з відповідного реченню вузла мережі. Природно, вага речень потім нормується, тому що довгі речення без цієї процедури в середньому будуть мати заздалегідь більшу вагу.

Особливості реферування правової інформації. Процедури автоматичного реферування екстрактного класу базуються на визначенні вагових значень (ступенем важливості) окремих речень, які, у свою чергу, залежать від вагових значень слів. У роботі в якості вагових значень слів використовувався класичний критерій *TF-IDF*, хоча це не єдиний можливий для вирішення завдання реферування підхід [7]. Традиційно для визначення вагових значень слів використовувалися два відомих алгоритма – у першому випадку вага речення розглядався як нормована по довжині цього речення сума вагових значень слів, що входять до нього, а у другому випадку використовувався, так званий, алгоритм симетричного реферування [8]. У цьому випадку вага речення визначається як сума вагових значень його зв’язків з попереднім і наступним реченнями.

Крім того, в даній роботі запропоновано мережевий алгоритм, в якому на відміну від другого випадку обчислюються зв’язки не тільки між сусідніми реченнями, а й між усіма реченнями у тексті документа. Такий підхід, звичайно, обчислювально більш складний, ніж перші два, однак, як показала практика, призводить до кращих результатів. При цьому складність алгоритму, в разі розглянутого підходу реферування текстів, наведених китайською мовою, компенсується тим, що замість слів (сегментація яких в даному випадку не потрібна) розглядаються лише окремі ієрогліфи.

Слід зазначити, що специфіка правової інформації, вимоги до структури і обсягу реферату, дозволили використовувати наведені вище універсальні підходи до вирішення окремої спеціальної задачі.

До структури і обсягу реферату правового документа (приклади таких документів можна знайти на сайті http://www.gov.cn в розділі /zhengce) висуваються вимоги, які знайшли свою програмну реалізацію:

1. Реферат починатися з заголовка документа, наведеного практично без змін.

2. У рефераті відзначається вид документа (оголошення “通告”, звіт “报告”, результати роботи “工作 成果”, положення “政策” тощо).

3. Якщо у документі позначена його мета (маркери: “目的”, “奖补目的”, “调整目的”, “普查的目的和意义” тощо), то вона також знаходить відображення у рефераті.

4. Якщо в першому або другому реченні документа позначені суб’єкти призначення документів (що також видно за спеціальними маркерами), то таке речення також включається до складу реферату.

5. Якщо в заголовку документа або в позначенні його мети в явному вигляді присутні об’єкти з числа заздалегідь відомих (що входять у таблицю базових об’єктів), то ці об'єкти повинні бути виділені в рефераті.

6. Якщо документ відноситься до типу, що не підлягає подальшому реферуванню (нагороди “表彰”, оголошення про торги “招标”, листи “函” і ін), то реферат також вважається підготовленим.

7. З тексту документа вибираються всі речення, що містять вибрані із заголовка і цілі об’єкти. Якщо таких речень менше необхідного числа (яке задається заздалегідь або розраховується виходячи з обсягу документа), то вони виводяться в реферати в тій же послідовності, що і в первинному документі. Реферат вважається підготовленим.

8. Якщо речень більше необхідного числа, то вони зважуються відповідно до наведеного вище алгоритму (за результатами тестування обрано мережевий алгоритм). Після цього речення ранжируються за вагою і необхідна їх кількість виводиться в реферат в тій же послідовності, що і в первинному документі. Реферат вважається підготовленим.

Згідно з наведеними вимогами була розроблена програма автоматичного реферування правової інформації, наданої китайською мовою.

Суміжні завдання Text Mining. Автоматичне реферування текстів – це одна з важливих задач технологій глибинного аналізу текстів (Text Mining), яка включає ще декілька напрямків, таких як витяг сутностей (Information extraction), побудова мереж слів (Language Networks), що відображають особливості предметних областей, кластеризації (Cluster Analysis).

Запропонований для реферування алгоритм спирається на деяку множину заздалегідь підготовлених слів, що відображають основні об’єкти, представлені в правових документах (наприклад, “人口” – населення, “产业” – промисловість, “儿童” – діти, тощо).

Разом з тим, якщо застосувати алгоритм сегментації слів, після чого їх ранжирувати, то легко можна виділити “розширення” стартових об’єктів, що найбільш часто зустрічаються, наприклад, поняття “організація” (组织) розширити до поняття “міжнародна організація” (国际 组织), “громадська організація” (社会 组织), а поняття “оборона” (事业) до поняття “народна протиповітряна оборона” (人民 防空 事业). У результаті документам масиву правової інформації були поставлені у відповідність основні поняття, які можуть виступати в якості “ключових слів”, дескрипторів, основ побудови моделей предметних областей (Subject Domain).

Як один з видів моделей предметних областей може розглядатися мережа слів, вузли якої відповідають окремим поняттям [9]. Були запропоновані і реалізовані такі прості правила побудови цієї мережі, тобто правила встановлення зв’язків між вузлами:

1. Всі об’єкти з базового, заздалегідь підготовленого списку, що входять в один документ зв’язуються зв’язками.
2. Якщо два об’єкти входять до N різних документів, то сила зв’язку між ними дорівнює N.
3. Поняття, що є розширеннями понять з стартового набору, зв’язуються з відповідними базовими поняттями.

За допомогою програми Gephi (http://gephi.org) [10] побудована мережа була візуалізована (Рис. 1) і були отримані такі парметри побудованої мережі: кількість вузлів – 3364 (кількість об’єктів з стартового набору – 220); кількість зв’язків – 10167; щільність мережі – 0.001; кількість зв’язаних компонент – 6; середня довжина шляху – 3.013; середній коефіцієнт кластеризації – 0.859.

До топологічної особливості побудованої мережі відноситься дуже великий середній коефіцієнт кластеризації. Це пояснюється, з одого боку, великою кількістю понять, пов’язаних лише з поняттям, що їх породжує (відсутність інших сусідів), а з іншого боку сильною зв’язністю об’єктів зі стартового списку. Невелика середня довжина шляху свідчить про те, що ця мережа є “малим світом” (Small World) [11].

Наведене на Рис. 1 та 2 загальний вигляд мережі слів наочно демонструє подальшу можливість кластеризації мережі, вибору підмножин – кластерів із слів (понять). Ця процедура дозволяє виділяти тематичні підмножини в рамках розглянутої предметної області.

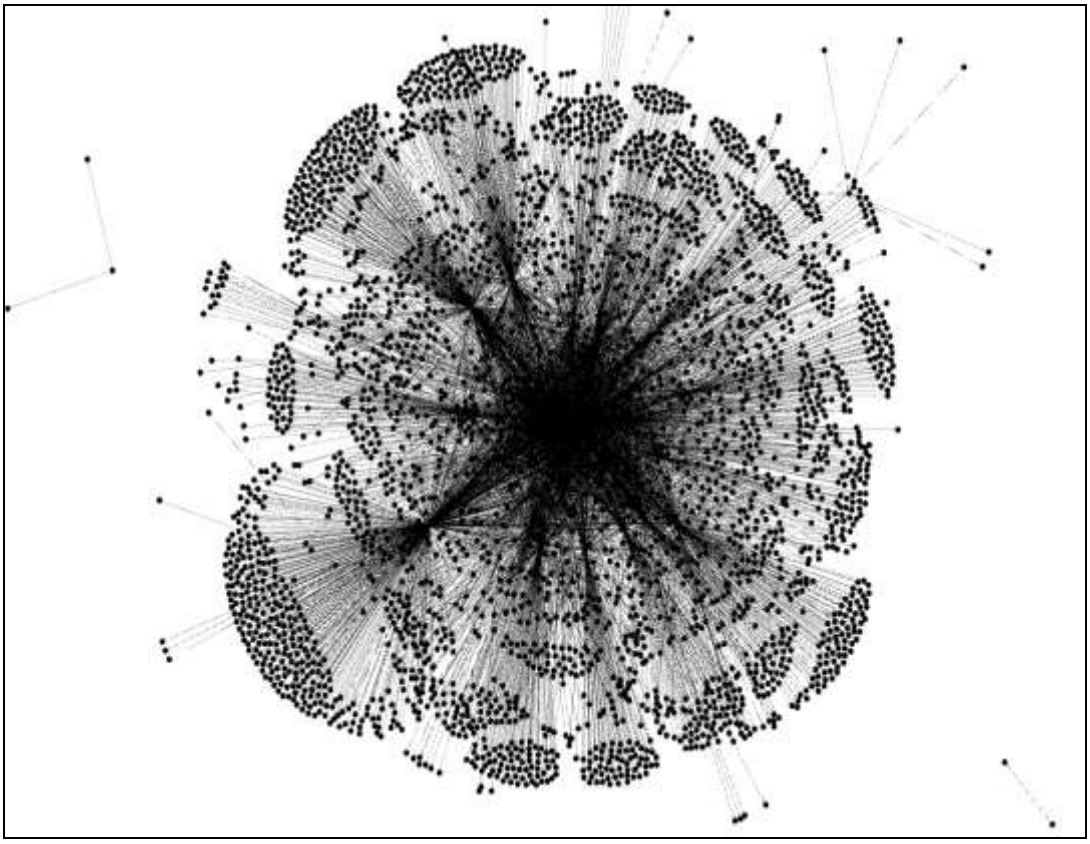
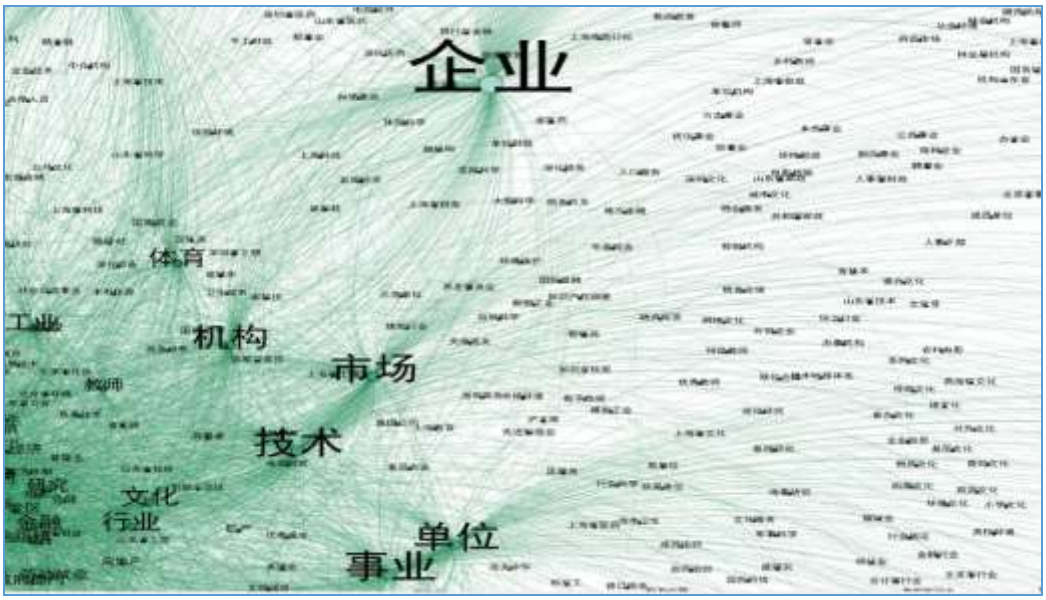


Рис. 1 – Загальний вигляд мережі слів



Фрагмент мережі слів

Рис. 2 – Мережа слів, що відображує предметну область

За допомогою програми Gephi також були отримані списки найбільш вагомих вузлів відповідно до мережевих рангових критеріїв PageRank і HITS [12] (Рис. 3).

Label	PageRank
水利	0.001548
“十一五”	0.00154
扶贫	0.00149
毕业生	0.001408
银行	0.001405
上海市财政	0.001383
邮政	0.001374
林业	0.001352
信息传输	0.001349
城市规划	0.001337
文物	0.001323
医生	0.001315
省财政	0.001242
技术服务	0.001215
山东省财政	0.001194
农民工	0.001126
县域	0.00111
农田	0.001097
电信	0.001072
经济特区	0.001055
科技创新中心	0.001045
试验区	0.001
北京市财政	0.000989
食品药品	0.000964
电影	0.000949
房地产	0.000897
矿产	0.00088
供销	0.000877

PageRank

Label	Hub
残疾人	0.04637
租赁	0.044748
科技创新中心	0.043809
农民工	0.043738
统计	0.04244
电信	0.04112
省财政	0.040688
经济特区	0.039118
山东省财政	0.039081
作业	0.038172
食品药品	0.036646
北京市财政	0.036476
水利	0.036002
试验区	0.035958
电影	0.031812
人工智能	0.031356
娱乐	0.03121
邮政	0.028793
物流业	0.027323
海关	0.026766
社会信用体系建设	0.026739
餐饮	0.02619
深圳市市场	0.02569
干部	0.025645
公共管理	0.025336
金融业	0.025252
食品药品监管	0.025083
经济体制	0.025021

HITS

Рис. 3 – Найбільш рейтингові слова за критеріями PageRank і HITS

Оцінювання результатів. Для оцінювання результатів застосовується дві оцінки якості реферату без участі експертів – косинусна міра і дивергенція Дженсена-Шеннона (Jensen-Shannon), обґрунтування застосування яких надано в роботі [13].

Строго кажучи, міра Дженсена-Шеннона відповідає втраті інформації при реферування і пропорційна сумарній вазі слів (в нашому випадку – ієрогліфів), що входять в документ, але відсутні в рефераті.

При реферування була реалізована нова ідея визначення вагових значень речень на основі вагових значень окремих ієрогліфів, а не слів, як це загальноприйняте. Тому якість реферування перевірялася не лише виходячи з урахування ваги окремих ієрогліфів, а й з урахуванням ваги цілих слів, що входять в документи і реферати, щоб переконатися, що запропонований підхід задовільний і за критеріями традиційних систем реферування. Природно, для цього довелося виконати витратну за ресурсами процедуру сегментації слів [14]. Слід зазначити, що дана процедура виконувалася виключно для перевірки якості алгоритмів реферування і не входить до складу самого алгоритму реферування.

Випробування проводилися на реальному масиві правової інформації Китайської народної республіки обсягом 10 тисяч документів.

Висновки.

Результати випробувань дозволяють резюмувати наступне:

1. В роботі представлена гібридна методика автоматичного реферування, що охоплює статистичні та маркерні методи, а також облік розташування речень у тексті правового документа. Запропонована модель реферату відображає інформаційну потребу замовників при роботі з правовою інформацією. Наведені підходи призводять до результатів, якість відповідає представленим на відомій конференції з аналізу текстів.

2. Реалізовано підхід до визначення вагових значень окремих ієрогліфів, а не сегментованих слів в тексті документів. Дана методика дозволяє уникати витратної процедури сегментування слів, необхідної для інших змістовних методів обробки текстів, наведених китайською мовою.

3. Реалізовано і випробувані різні методи автоматичного реферування. Реферування на основі мережевої моделі документа виявилося кращим за критеріями косинусної міри і відстані Дженсена-Шеннона для рефератів, обсяг яких перевищує 2 речення.

4. Запропонований підхід з урахуванням змін в маркерах-шаблонах може використовуватися не тільки для правових документів, а й для текстів довільної тематики, зокрема, науково-технічної та новинної інформації.

Використана література

1. Luhn Hans Peter. The automatic creation of literature abstracts // IBM Journal of research and development. – 1958. – № 2. – Pp. 159-165.

2. Zhang C. Automatic Keyword Extraction from Documents using Conditional Random Fields // Journal of Computational Information Systems. – 2008. – № 4 (3). – Pp. 1169-1180.

3. Ramos J. Using tf-idf to determine word relevance in document queries / Proceedings of the first instructional conference on machine learning, 2003. – Pp. 1-4.

4. Bhart, Santosh Kumar, Babu Korra Sathya, Pradhan, Anima. Automatic Keyword Extraction for Text Summarization in Multi-document e-Newspapers Articles // European Journal of Advances in Engineering and Technology. – 2017. – 4 (6). – Pp. 410-427.

5. Chien L.-F. Pat-tree-based keyword extraction for Chinese information retrieval / ACM SIGIR Forum. 31, ACM, 1997. – Pp. 50-58.

6. Salton G., Buckley C. Term-weighting approaches in automatic text retrieval / Information Processing & Management. – 1998. – 24(5). – Pp. 513-523.

7. Lande D.V., Snarskii A. A, Yagunova E.V., Pronoza E. V. The Use of Horizontal Visibility Graphs to Identify the Words that Define the Informational Structure of a Text / 12th Mexican International Conference on Artificial Intelligence, 2013. – Pp. 209-215. DOI: 10.1109/MICAI. 2013.33

8. Яцко В.А. Симметричное реферирование : теоретические основы и методика // Научно-техническая информация. – (Серія 2). – 2002. – № 5. – С. 18-28.

9. Ланде Д.В. Елементи комп’ютерної лінгвістики в правовій інформатиці. – К. : НДІІП НАПрН України, 2014. – 168 с. ISBN 978-966-2344-33-2

10. Cherven Ken. Network Graph Analysis and Visualization with Gephi. – Packt Publishing, 2013. ISBN: 9781783280131

11. Kleinberg J. Navigation in a small world // Nature. – 2000. – № 406 (6798). – Pp. 845. DOI: 10.1038/35022643

12. Langville Amy N., Meyer Carl D. Google’s PageRank and beyond: the science of search engine rankings. – Princeton university press, 2011. ISBN: 9780691152660

13. Louis Annie, Nenkova Ani. Automatic Summary Evaluation without Human Models / In First Text Analysis Conference (TAC’08). – Gaithersburg, MD, Etats-Unis, 17-19 November 2008.

14. Berezin Boris A., Lande Dmitry V., Pavlenko Oleh Y. Development, Evaluation and Usage of Word Segmentation Algorithm for National Internet Resources Monitoring Systems / CEUR Workshop Proceedings, 2017. Selected Papers of the XVII International Scientific and Practical Conference on Information Technologies and Security (ITS 2017). – 2067. – Pp. 16-22.

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

УДК 342.9(004.9)

КОСТЕНКО О.В., головний науковий співробітник Інституту спеціальної техніки та судових експертиз Служби безпеки України

ЕЛЕКТРОННИЙ ПІДПИС ТА ЕЛЕКТРОННІ ДОВІРЧІ ПОСЛУГИ В ЗАКОНОДАВСТВІ СПОЛУЧЕНИХ ШТАТІВ АМЕРИКИ

Анотація. *У статті проаналізовано досвід Сполучених Штатів Америки щодо законодавчого регулювання правовідносин в сфері електронного підпису та електронних довірчих послуг. Досліджено основні напрямки правового впорядкування проблем застосування електронних підписів та їх сертифікатів, а також взаємного визнання вказаних послуг. Надано рекомендації щодо стандартизації правових норм під час взаємного визнання довірчих послуг між США та Україною.*

Ключові слова: *електронний підпис, сертифікат, електронні довірчі послуги, транскордонний режим електронних довірчих послуг, визнання іноземних сертифікатів електронних підписів.*

Summary. *The article analyzes the experience of the United States of America in the legal regulation of electronic signatures and electronic trust services. The main directions of legal regulation of the problems related to use of electronic signatures and their certificates, as well as the mutual recognition of these services, are investigated. Recommendations on standardization of legal norms during mutual recognition of trust services between the United States and Ukraine are provided.*

Keywords: *electronic signature, certificate, electronic trust services, cross-border electronic trust services, recognition of foreign certificates of electronic signatures.*

Аннотация. *В статье проанализирован опыт Соединенных Штатов Америки в отношении законодательного регулирования правоотношений в сфере электронной подписи и электронных доверительных услуг. Исследованы основные направления правового разрешения проблем применения электронных подписей и их сертификатов, а также взаимного признания указанных услуг. Даны рекомендации по стандартизации правовых норм во время взаимного признания доверительных услуг между США и Украиной.*

Ключевые слова: *электронная подпись, сертификат, электронные доверительные услуги, трансграничный режим электронных доверительных услуг, признания иностранных сертификатов электронных подписей.*

Постановка проблеми. За останні десятиріччя процеси глобалізації світової економіки завдяки інтеграції інформаційних технологій стрімко прискорили інформаційні процеси у всіх сферах діяльності громадян та держав, в тому числі обміну електронними послугами, розвитку електронної комерції, систем електронної освіти, здоров’я, банкінгу із застосуванням електронного підпису.

Законодавство іноземних країн в сфері електронного підпису має суттєві відміни як у понятійно-категорійному апараті і правових підходах застосування електронних підписів та довірчих послуг, в тому числі і в транскордонному режимі. Проблема правового регулювання визнання іноземних електронних довірчих послуг та транскордонного визнання сертифікатів електронних підписів є наразі актуальною.

Результати аналізу наукових публікацій. Вітчизняні та закордонні науковці досить широко вивчають практику застосування електронного підпису під час надання електронних довірчих послуг, однак їх увага переважно концентрується на формулюванні технічних або технічно-юридичних норм. В той же час комплексні дослідження,

присвячені саме проблемі правового регулювання визнання іноземних довірчих послуг та транскордонного визнання сертифікатів електронних підписів практично відсутні.

Вказаними питаннями правового регулювання суспільних відносин, пов’язаних з використанням електронного підпису займались: Бачило І., Семілєтов С., Локшин А., Перевозчикова О., Бєлов С., Горбенко І., Потій О., Тірі А., Elgar E., Faye F., Guercio T.C., Kinsella S., Laudon K. та інші. Незважаючи на наявність наукових напрацювань в сфері електронного підпису, питання вдосконалення правового регулювання електронних довірчих послуг та транскордонного визнання сертифікатів електронних підписів потребує подальшої наукової уваги.

Метою статті є порівняння базових понять законодавства та розгляд механізмів, які регулюють суспільні відносини в сфері електронного підпису та електронних довірчих послуг, в Сполучених Штатах Америки.

Виклад основних положень. На міжнародному рівні роботу із формування нових правових норм та нормативно-правових актів в галузі електронного обміну даними, електронної торгівлі та електронного цифрового підпису першою розпочала Комісія ООН з міжнародного торговельного права, порушивши у 1984 році на 17-й сесії Міжнародної торгової палати і Європейської економічної комісії (UNCITRAL) питання правових аспектів застосування електронних документів та їх юридичної сили. Це спонукало до роботи із правової стандартизації в галузі електронної торгівлі та електронного цифрового підпису не тільки міжнародні організації та об’єднання (союзи) але й низку країн.

Сполучені Штати Америки активно розпочали законотворчу діяльність в сфері електронного підпису і стали першою країною, яка запровадила електронний (цифровий) підпис в якості аналога власноручного підпису.

1 травня 1995 року штатом Юта вперше у Сполучених Штатах Америки запроваджено Закон “Про цифровий підпис” (Utah Digital Signature Act) [1], який став основою законодавства в галузі електронного підпису та електронних послуг. Звичайно США вже використовували електронні підписи в комерційній та банківській діяльності, однак їх правове регулювання розпочалося саме із законодавства штату Юта. За первинним задумом Закон “Про цифровий підпис” мав на меті мінімізувати випадки підробки цифрового підпису, надати можливості для доказу автентичності інформації в електронній формі, а вже потім сприяти використанню цифрового підпису для засвідчення електронних документів та спрощення процедури здійснення комерційних угод в електронному вигляді.

Закон штату Юта “Про цифровий підпис” запровадив визначення не електронного, а саме “цифрового підпису” (digital signature), який визначається як “послідовність бітів”, що отримана підписувачем в результаті проходження “повідомлення” (message), яке підписується через однобічну функцію, а потім процедуру шифрування за допомогою асиметричного криптографічного алгоритму і “закритого ключа”. Закон також дає визначення понять “закритий ключ”, “відкритий ключ”, “підписувач” та “сертифікат підписувача”, а також запроваджує правові підстави функціонування засвідчувального центру Міністерства комерції штату Юта та регламентує створення інфраструктури, яка забезпечить надійне та ефективне використання цифрового підпису.

Вперше в законодавстві США нормативно-правовим актом встановлюється норма, згідно якої документ, підписаний за допомогою цифрового підпису, набуває однакової юридичної сили з паперовим документом, підписаним власноручним підписом особи. В той же час закон не надає безпосередньо визначень електронних або цифрових послуг, а також не регламентує процедур визнання іноземних сертифікатів, покладаючи ці

функції, а рівно як і доказування юридичної їх надійності, на сторони комерційної або іншої правової угоди.

У жовтні 1995 року штат Каліфорнія прийняв Закон “Про цифровий підпис” (California Digital Signature Act) [2]. Зазначений нормативно-правовий акт, на відміну від Закону штату Юта, був створений для регулювання правовідносин, які виникають під час застосування електронних підписів в державному секторі між громадянами і державними органами. Закон штату Каліфорнія має суттєві розбіжності у базових визначеннях поряд з Законом штату Юта, тобто надає власні редакції дефініціям “цифровий підпис”, “повідомлення”, “особа”, “підписувач” та інші. Також, вперше вводиться поняття “ключова пара”, що означає приватний ключ та відповідний його відкритий ключ у асиметричній криптосистемі. Як і попередній Закон штату Юта, Закон штату Каліфорнія не надає визначень електронних або цифрових послуг, а процедури визнання сертифікатів, в тому числі і іноземних, ґрунтується на необхідності створення цифрового підпису за технологією, прийнятною для використання штатом Каліфорнія.

В березні 1996 року штатом Нью-Мексико прийнято Закон “Про електронну аутентифікацію документів” (Electronic Authentication of Documents Act). Мета закону – створення централізованого, загальнодоступного електронного реєстру для аутентифікації електронних документів за допомогою системи відкритого та закритого ключів, спрощення процесу обміну електронними документами та іншою інформацією при укладанні комерційних угод. На відміну від поняття “електронний” або “цифровий підпис” законотворцями запропоновано визначення “електронна аутентифікація” (electronic authentication), яке трактується як “електронне підписання документа, що встановлює гарантований зв’язок між автором документа і самим документом за допомогою системи відкритого та закритого ключів”.

Нововведенням можна вважати введення окремого розділу “Повноваження і обов’язки Центру електронної документації”. Вперше в законодавстві запроваджується Реєстр відкритих ключів для перевірки аутентичності електронних підписів, створених відповідно до стандартів, а також, відкритих ключів державних установ, фізичних осіб, які мають ділові відносини з державними структурами та інших осіб, реєстрація яких може бути здійснена за законом.

Розглядаючи Закон штату Вашингтон “Про електронну посвідчення документів” (Washington Electronic Authentication Act) [3], прийнятий 29 березня 1996 року, констатуємо таку ж мету, що і в Законі штату Юта. Однак Законом штату Вашингтон закріплюється одночасно вся група основоположних понять, використана раніше законодавцями штатів Нью-Мексико, Каліфорнія та Юта, до яких відносяться: “повідомлення”, “цифровий підпис”, “відкритий і закритий ключі”, “сертифікат”, “засвідчувальний центр”. Закон штату Вашингтон прирівнює цифровий підпис до власноручного підпису за умови, що його справжність підтверджена за допомогою відкритого ключа, відображеного в сертифікаті. Цікавим нововведенням є положення про те, що копія електронного документа, завірена підписом має однакову юридичну силу з оригіналом за винятком випадків, коли автор документа наділяє оригінал унікальною юридичною силою.

У травні 1996 року прийнято Закон штату Флорида “Про електронний підпис” (Florida Electronic Signature Act) [4]. Як і в Законі штату Нью-Мексико, закон має загальну сферу застосування. Крім того, законодавці штату Флорида пропонують використовувати термін writing (“написання”) не тільки в значенні написати що-небудь на папері, а й для позначення “процесу створення електронного документа на будь-якому носії з можливістю подання його в загальноприйнятій формі”, що законодавчо

закріплює єдиний загальний термін для позначення і електронного і традиційного паперового документа. У Законі штату Флорида вперше були запропоновані одразу обидва визначення: “електронний підпис” і “цифровий підпис”. “Електронний підпис” (electronic signature) трактується як більш широке поняття – це “будь-які літери або символи, створені електронними засобами, що дозволяють підтвердити авторство і справжність документа або спростувати їх”. “Цифровий підпис” (digital signature) трактується як “різновид електронного підпису, який перетворює повідомлення, використовуючи асиметричний криптографічний алгоритм таким чином, що одержувач повідомлення, маючи відкритий ключ, може визначити: чи було повідомлення спочатку зашифровано з використанням відповідного закритого ключа і чи було повідомлення змінено з моменту перетворення (шифрування)”. Ключовим моментом Закону штату Флорида є положення яким електронний підпис наділяється рівнозначною юридичною силою з власноручним підписом і дозволяється його використання для підписання документів.

17 березня 1997 штатом Міссісіпі прийнято Закон “Про цифровий підпис” (Digital Signature Act of 1997), який дозволив використання цифрових підписів для підписання електронних документів в комерційній діяльності і законодавчо закріпив весь перелік основних понять попередніх законів. Крім визначення терміну “цифровий підпис” закон пропонує і загальне визначення терміну “підпис”, який розуміється як “будь-яка послідовність слів, букв, символів, імен, назв, включаючи торгові марки, створена від руки, за допомогою спеціальних пристроїв, електронних або інших засобів з наміром підтвердити справжність документа”. Питання надання цифровому підпису юридичної сили вирішене традиційно – цифровий підпис, справжність якого засвідчена, може використовуватися для підписання електронного документа і буде мати однакову юридичну силу з власноручним підписом.

Практично одночасно, в квітні 1997 року, прийнято Закон штату Джорджія “Про електронний документ і електронний підпис” (Georgia Electronic Records and Signatures Act, Senate Bill № 103) [5]. Основним завданням закону вважалося законодавче закріплення використання електронних документів та електронних підписів в різних сферах діяльності суспільства. Тому можна зробити висновок про те, що творці закону не обмежили сферу його застосування, а загальні визначення, в тому числі і електронного підпису, не закріплюють будь-яку певну технологію створення електронних документів та електронних підписів.

Цікавим рішенням є закріплення на законодавчому рівні основних напрямків політики штату для розвитку електронної комерції і заохочення ведення бізнесу за допомогою електронних засобів зв’язку. Так, всі державні установи спільно з приватними організаціями зобов’язані були створювати бізнес-проекти (startup) для вивчення можливостей застосування нових інформаційних технологій (в тому числі, і технологій електронного підпису). Такий підхід сприяв легалізації використання електронних документів та електронних підписів, але не наполягав на використанні будь-якої однієї технології.

Штат Міннесота у травні 1997 року запроваджує Закон “Про електронну аутентифікацію документів” (Minnesota Electronic Authentication Act) [6]. Новизна даного нормативного акту полягає в тому, що разом із традиційною метою спрощення процедури укладення комерційних угод за допомогою використання електронних документів, декларується потреба створення спільно з іншими штатами США універсальних правил, що регулюють питання використання електронних документів. Закон штату Міннесота цікавий тим, що фактично запроваджує основи створення

інфраструктури відкритих ключів (Public Key Infrastructure – PKI). Законом закладаються правові основи роботи центрів, що надають послуги електронних підписів, такі як: процедура отримання ліцензії; функціональні обов’язки засвідчувального центру; процедури призупинення дії, відновлення або відкликання ліцензії; відповідальність, яку несуть ліцензовані засвідчувальні центри за невиконання положень цього закону. Закон штату Міннесота більш суворо підходить до питання юридичної сили цифрового підпису.

Практично одночасно із штатом Міннесота, в червні 1997 року, штатом Індіана прийнято Закон “Про електронний цифровий підпис” (Electronic Digital Signature Act) [7], який закріпив право державних установ використовувати цифровий підпис для укладення угод в електронній формі за винятком Казначейства, Верховного Суду та юридичних, законодавчих, і аудиторських організацій. Сфера застосування електронного підпису була обмежена державними установами. Такий підхід вже зустрічався в Законі штату Каліфорнія, але без позначення обмежень. Також, як і в Законі штату Флорида, використовується одночасно два терміни: “електронний підпис” і “цифровий підпис”. Однак Законом штату Індіана перевагу все ж надано саме цифровому підпису. Необхідною умовою володіння юридичною силою для цифрового підпису, приєднаного до вихідних і вхідних електронних документів державних установ є його відповідність конкретним критеріям за Законом штату Індіана.

В цей же час, в червні 1997 року, штатом Техас прийнято Закон “Про електронний підпис” (Texas House Bill 984). Сфера застосування положень даного закону обмежена діяльністю державних організацій, що отримали право використання електронних документів, які вважалися підписаними і володіли відповідною юридичною силою, за наявності в якості реквізиту цифрового, а не електронного підпису. Цифровий підпис використовувався для посвідчення електронних документів, які надсилаються в державні організації. Юридична сила цифрового підпису визначалася його відповідністю набору критеріїв, як і в Законі штату Індіана.

В кінці липня 1997 року штатом Орегон прийнято Закон “Про електронний підпис” (Electronic Signature Act, 1997 Oregon House Bill) [8]. Сфера дії цього закону така ж, як у розглянутого раніше Закону штату Техас, і була обмежена діяльністю державних установ при обміні електронними документами. Нововведенням можна вважати запровадження нової дефініції – key pair (“ключова пара”), яка складається із закритого ключа і відкритого ключа. Законом також була встановлена необхідність створення системи центрів, що засвідчують та видають сертифікати, визначено уповноважену особу, яка відповідає за реєстрацію та сертифікацію засвідчувальних центрів.

У квітні 1998 року штатом Небраска прийнято Закон “Про цифровий підпис” (Digital Signature Act, Nebraska Revised Statutes), який дозволив використання цифрового підпису для засвідчення документів в різних областях суспільної діяльності. Центральним поняттям закону є саме цифровий підпис, визначення якого достатньо унфіковане: “цифровий підпис – це електронний ідентифікатор, що створений комп’ютером і використовується підписувачем в якості власноручного підпису”. Таке визначення спрощує технологічний підхід побудови інфраструктури відкритих ключів.

У вересні 1999 року прийнято Закон штату Нью-Йорк “Про електронні документи та електронний підпис” (Electronic Signatures and Records Act, Chapter 57-A of the Consolidated Laws, State Technology Law Sections) [9].

Серед всієї сукупності розглянутих законів окремих штатів Закон штату Нью-Йорк насамперед цікавий тим, що він містить визначення поняття термін “електронний”, що включає в себе “цифровий, магнітний, бездротовий, оптичний, електромагнітний і

інший”, а також визначення електронного підпису “електронний ідентифікатор, що включає в себе і поняття цифрового підпису, який є унікальним для його підписувала, справжність якого може бути підтверджена і який перебуває під особистим контролем підписувача та який приєднаний до підписаних даних таким чином, що можна відстежити зміни документа, зроблені після підписання, а також передбачається, що підписувач наділяє його однаковою силою з власноручним підписом”.

Закон штату Нью-Йорк вперше гарантував громадянам можливість використовувати електронні документи та електронний підпис в якості доказу в суді (за винятком окремих випадків) нарівні з паперовими документами.

Протягом 5 років Сполучені Штати Америки активізували законотворчу діяльність з метою впорядкування суспільних відносин, які виникали разом із розвитком інформаційних технологій, електронної комерції, структури відкритих ключів PKI. Наслідком цієї діяльності стали чисельні нормативні акти в сфері електронного підпису, електронного документу та електронної комерції, що поставило проблему уніфікації правової бази та урегулювання питань термінології та окремих норм права, в тому числі порядку визнання іноземних сертифікатів електронних підписів. Проблема була вирішена розробкою федеральних законодавчих актів – Модельного закону “Про електронні угоди” (Uniform Electronic Transactions Act – UETA) [10] та Федерального закону США “Про електронні підписи в міжнародних і внутрішньодержавних торгових відносинах” (Electronic signature global and national act. Public law 106-229-2000) [11].

Одним із принципових положень Модельного закону “Про електронні угоди” є норма, згідно якої визнання дійсності електронних угод, електронних документів, електронних підписів та їх сертифікатів можливі за згодою сторін, що беруть участь у обміні електронними документами. Фактично держава відходить від регулювання процедури визнання електронних послуг, електронних підписів та сертифікатів і покладає це на суб’єктів-учасників правовідносин. Слід зазначити, що даний закон дотепер не підтримали штати Вашингтон, Іллінойс та Нью-Йорк.

Федеральний закон США “Про електронні підписи в міжнародних і внутрішньодержавних торгових відносинах” прийнятий Конгресом США 24 січня 2000 року. Цікаво відзначити, що Президент публічно підписав Федеральний закон “Про електронний підпис в міжнародних і внутрішньодержавних торгових відносинах” саме за допомогою електронного підпису.

Після прийняття федерального закону електронний підпис вже може легально використовуватися сторонами угоди. Визначення електронного підпису в законі є технологічно нейтральним і містить лише основну ідею та поняття, надаючи в подальшому фахівцям можливість вибору оптимальної технології для розвитку інфраструктури електронного підпису. Федеральний закон США встановив на державному рівні рівнозначність електронного документа та електронного підпису нарівні з паперовими документами та власноручним підписом. Виняток склали лише деякі види документів: заповіти, свідоцтва про шлюб, розлучення, усиновлення та інші акти цивільного стану; документи, що містять рішення суду, протоколи; документи про нерухомість, комунальні послуги; медичні документи, наприклад, страховка і деякі інші. Питання визнання сертифікатів вирішується однаково для внутрішньодержавних і для міжнародних торгових операцій – за попередньою згодою сторін угоди та за умови, що електронні підписи відповідають вимогам законодавства.

Окремо слід звернути увагу на численні розбіжності в законодавстві, що призводять до виникнення складнощів адаптації стандартів електронних підписів та документів окремих штатів. З метою запровадження уніфікації в галузі електронного

підпису в США законодавством рекомендується використовувати стандарт X.509 з мінімальними змінами та максимально використовувати механізми розширень сертифіката федерального профілю, який розроблено Національним інститутом стандартів и технологій США (The National Institute of Standards and Technology – NIST) Міністерства торгівлі США у співпраці із та Американським національним інститутом стандартів (ANSI). Також, цими установами розроблено федеральний міст сертифікації (Federal Bridge Certification Authority – FBCA), який має за мету об’єднати відомчі інфраструктури відкритих ключів (PKI) США, а також формувати сертифікати, що є дійсними для PKI одного відомства, та які будуть прийнятими в PKI іншого відомства, за умови що відомства укладають угоду про те, що їх відомчі PKI зв’язуються через FBCA. Фактично FBCA забезпечує інтероперабельність електронних підписів в межах США шляхом трансляції інформації із відомчих сертифікатів в загальний сертифікат, який буде прийнятним для інших учасників сертифікації. Однак даним технічним рішенням ніяким чином не вирішуються проблеми визнання в США іноземних електронних підписів та електронних довірчих послуг.

На прикладі цих законів ми могли простежити за досвідом США у сфері правового регулювання електронних документів та електронного цифрового підпису. Американськими фахівцями була проведена велика робота, оскільки практично в кожному штаті були прийняті основні закони по даній темі, а також різні доповнення та поправки у вигляді Правил, Інструкцій або нових версій існуючих законів.

Висновки.

Узагальнюючи законодавчий досвід США, який регулює використання електронних документів і електронного підпису, можна констатувати наступне.

Законодавча база США, яка регулює використання електронного підпису, створюється поступово із застосуванням підходу “від часткового до загального”, тобто, від створення законопроектів і прийняття законів в окремих штатах до створення Федерального закону.

Законодавцями США була зроблена спроба використання протилежного підходу – “від загального до конкретного” – шляхом розробки Модельного закону “Про електронні угоди” (UETA) для подальшого створення в усіх штатах локальних законів на його основі. Ця спроба виявилася вдалою, і вже до червня 2002 року в 39 штатах були прийняті закони “Про електронні угоди”, що регулюють питання використання електронних документів та електронних підписів в певній сфері діяльності – електронній комерції.

Що ж стосується порушеного дослідженням питання щодо визнання іноземних електронних підписів, сертифікатів електронних підписів, електронних довірчих послуг, то ці проблемні питання законодавством США не вирішуються окремо або детально – відсутні визначення транскордонності, електронних довірчих послуг та їх перелік, а також порядок або процедури визнання іноземних електронних підписів та їх сертифікатів під час транскордонних відносин, в тому числі в електронній комерції. Законодавство США не передбачає інших процедур визнання іноземних сертифікатів ніж за попередньою згодою сторін-учасників угод та за умови, що електронні підписи були створені і відповідають вимогам законодавства.

Таким чином при забезпеченні процедур взаємного визнання електронного підпису та електронних довірчих послуг між США та Україною законотворцям необхідно розробити та стандартизувати правові механізми транскордонного використання електронного підпису та електронних довірчих послуг із урахуванням особливостей різних технічних рішень та відмінностей юрисдикцій.

Використана література

1. Utah Digital Signature Act / Utah Code §§ 46-3-101 to 46-3-504 Enacted by L. – 1995, ch. 61. URL: http://www.jus.unitn.it/USERS/PASCUZZI/privcomp97-98/documento/firma/utah/udsa.html (дата звернення 18.06.2018).

2. Digital Signatures. – 1995. URL: http://www.sos.ca.ov/administration/regulations/current-regulations/technology/digital-signatures/ (дата звернення 18.06.2018).

3. WASHINGTON ELECTRONIC AUTHENTICATION ACT. – 1996. URL: http://apps.leg.wa.gov/rcw/default.aspx?cite=19.34 (дата звернення 18.06.2018).

4. The Electronic Signature Act of 1996: B reaking Down Barriers to Widespread Electronic Commerce in Florida / Florid a State Universit y Law Review. – 1997. URL: https://ir.law.fsu.edu/cgi/viewcontent.cgi?referer=; https://www.google.com/&httpsredir=1&article =1435&context =lr (дата звернення 18.06.2018).

5. Electronic Records and Signatures Act / SB 103 97 SB103/AP SENATE BILL 103. – 1997. URL: http://www.legis.ga.gov/Legislation/Archives/19971998/leg/fulltext/sb103.htm (дата звернення 18.06.2018).

6. ELECTRONIC AUTHENTICATION / State of Minnesota. CHAPTER 325K. – 1998. URL: https://www.revisor.leg.state.mn.us/statutes/?id=325K (дата звернення 18.06.2018).

7. Electronic and Digital Signatures / Indiana State Board of Accounts. – 1997. URL: https://www.in.gov/sboa/3232.htm (дата звернення 18.06.2018).

8. The electronic Signature Act / Legislative Administration Committee, Policy and Research Office. – 1997. URL: http://library.state.or.us/repository/2010/201010061538333/1997.pdf (дата звернення 18.06.2018).

9. Electronic Signatures and Records Act (ESRA) / New York State. – 1999. URL: https://its.ny.gov/electronic-signatures-and-records-act-esra (дата звернення 18.06.2018).

10. UNIFORM ELECTRONIC TRANSACTIONS ACT / NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS. – 1999. URL: http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf (дата звернення 18.06.2018).

11. ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT / PUBLIC LAW 106-229. – 2000. URL: http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (дата звернення 18.06.2018).

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

Інформаційна і національна безпека

УДК 340:351.86

БОГУЦЬКИЙ П.П., *кандидат юридичних наук, доцент,* головний науковий співробітник наукового центру правового забезпечення інформаційної і національної безпеки НДІ інформатики і права НАПрН України

ПОНЯТТЯ ТА ОЗНАКИ ПРАВА НАЦІОНАЛЬНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *Висвітлено концептуальні визначення права національної безпеки та його місця у системі права України, наведено ознаки, характеристику об’єктів та суб’єктів права національної безпеки, визначено зміст правовідносин у сфері національної безпеки. Вказано функції і принципи права національної безпеки та системної цілісності правових норм задля досягнення безпечних умов життєдіяльності людини, суспільства і держави. Зазначено, що право національної безпеки консолідує норми Конституції і законодавства України, у т.ч. норми інформаційного, адміністративного, екологічного та інших галузей, які стосуються забезпечення національної безпеки. У емпіричному та онтологічному значеннях право національної безпеки розглядається як галузь юридичної науки, навчальної дисципліни та законодавства.*

Ключові слова: *право національної безпеки, суб’єкти, об’єкти права національної безпеки, функції права, правовий режим, принципи права національної безпеки.*

Summary. *The article deals with the question of determining the law of national security in the system of law of Ukraine. The signs of the national security law as a complex branch are presented, the characteristics of objects and subjects of the national security law are described, the content of legal relations in the sphere of national security is determined. Attention is paid to the functions and principles of the national security law. It is established that the national security law forms the systemic integrity of legal norms through the action of the legal regime in relation to the achievement of the goal - safe living conditions of a person, the existence of society and the state. The national security law consolidates the norms of the Constitution and legislation on national security, as well as the norms of administrative, military, environmental, information, etc. branches of law directly related to the provision of national security. The most stable relationship is the law of national security and military law. The national security law, having the features of a complex branch of law, is considered empirically and ontologically relevant as industry of legislation, as a branch of legal science, and as an educational discipline.*

Keywords: *the national security law, subjects and objects of national security law, the functions of law, the legal regime, the principles of the national security law.*

Аннотация. *Исследованы концептуальные определения права национальной безопасности и его места в системе права Украины, приведены признаки, характеристика объектов и субъектов права национальной безопасности, определено содержание правоотношений в сфере национальной безопасности. Указаны функции и принципы права национальной безопасности и системной целостности правовых норм для достижения безопасных условий жизнедеятельности человека, общества и государства. Отмечено, что право национальной безопасности консолидирует нормы Конституции и законодательства Украины, в т.ч. нормы информационного, административного, экологического права и других отраслей, связанных с обеспечением национальной безопасности. В эмпирическом и онтологическом значениях право национальной безопасности рассматривается как отрасль юридической науки, учебной дисциплины и законодательства.*

Ключевые слова: *право национальной безопасности, субъекты, объекты права национальной безопасности, функции права, правовой режим, принципы права национальной безопасности.*

Постановка проблеми. Право національної безпеки України є однією з актуальних проблем сучасної юриспруденції, що вимагає комплексного наукового опрацювання з метою встановлення емпіричних основ, визначення певної множинності норм у системі права, які мають свою сферу дії [1]. Це потребує наукового обґрунтування власної предметності, змісту, функцій та місця у системі права.

Емпірична основа права національної безпеки – уся сукупність складних і важливих для сьогодення соціальних чинників, які забезпечують безпеку людини, суспільства і держави в умовах, що характеризують глобалізаційні процеси [2]. Національна безпека для України, як і для кожного сучасного суспільства та кожної держави, є проблемою, вирішення якої дозволяє існувати у соціальному просторі на основі сталого розвитку в усіх сферах людського буття [3, с. 78-86].

Для українського суспільства проблема національної безпеки в сучасних умовах є надзвичайно актуальною, що обумовлено необхідністю захисту суверенітету і територіальної цілісності держави від посягань на конституційний лад від зовнішньої воєнної агресії [4].

Також варто констатувати відсутність цілісної концепції права національної безпеки України. Такі концептуальні розробки присутні у багатьох правових системах, де безпекові проблеми вирішені або успішно вирішуються з урахуванням міжнародно-правових вимог.

Насамперед, будь-які розробки проблем права національної безпеки мають враховувати пріоритетність правового забезпечення національної безпеки, що відповідає, власне, призначенню права. При цьому, правове забезпечення національної безпеки виявляється на різних інституційних та функціональних рівнях, у різних сферах і галузях, маючи у своїй основі певні правові моделі. Для України актуальним є використання найбільш ефективного правового забезпечення національної безпеки, яке існує у країнах, що належать до НАТО, насамперед, це стосується правової моделі національної безпеки США [5]. Право національної безпеки тієї чи іншої держави, і Україна тут не є винятком, має враховувати особливості національних суспільних відносин, які склалися і формуються в межах існуючої правової системи, та в основі яких знаходяться економічні, політичні, воєнні, інформаційні, техногенні та інші характеристики. Такі характеристики або ж показники не можуть бути повторенням тих, що існують в інших правових системах. Їх врахування та використання є обов’язковими, оскільки національна безпека, а отже і право національної безпеки, формуються у межах міжнародного правопорядку. Найбільш важливими є взаємозв’язки права національної безпеки з військовим правом, що спонукає до об’єднання доктринальних розробок, до формування спільних підходів у правотворчості та у правозастосуванні.

Результати аналізу наукових публікацій. Наукові публікації проблем національної безпеки України представлені в юридичній науці численними розробками. Упродовж тривалого періоду вітчизняними науковцями здійснено філософсько-правові й теоретичні дослідження у сфері національної безпеки (О.Г. Данильян, О.П. Дзьобан, М.І. Панов, С.І. Максимов, Н.Р. Нижник, В.Г. Пилипчук та ін.); конкретно-наукові розробки з проблем національної безпеки (О.С. Власюк, В.П. Горбулін, Г.П. Ситник, А.П. Качинський, В.В. Крутов, Ю.В. Нікітін, В.Л. Федоренко та ін.). Досліджено загальнотеоретичні аспекти стійкості держави (Ю.М. Оборотов) і правового порядку (А.Ф. Крижановський), правові аспекти національних інтересів (П.П. Гай-Нижник, С.І. Пирожков, Л.В. Чупрій та ін.), адміністративно-правові особливості формування внутрішньої безпеки (В.Я. Настюк, Г.О. Пономаренко,), теоретичні та прикладні аспекти кримінально-правової охорони національної безпеки (В.В. Кузнецов, О.А. Чуваков).

Ґрунтовні правові дослідження проведено у різних галузях національної безпеки. Зокрема, важливого значення набувають розробки проблем інформаційної безпеки, проведені В.М. Брижком, О.Д. Довганем, О.О. Золотар, В.Г. Пилипчуком, В.М. Фурашевим та іншими вченими, кримінально-правової охорони інформаційної безпеки (М.В. Карчевський, Н.А. Савінова). Більш ефективних якісних ознак набули дослідження правових основ воєнної безпеки (В.К. Антошкін, О.В. Кривенко, В.В. Петров, А.О. Пелих Є.Л., Стрельцов та ін.). Послідовними є дослідження правових проблем національної безпеки і військового права, які проводить І.М. Доронін. Засадничі питання правових основ національної безпеки, розроблені В.Г. Пилипчуком та М.П. Стрельбицьким, наразі дають змогу вийти на новий рівень дослідження права національної безпеки, визначившись з відповідною науковою спеціалізацію – “право національної безпеки; військове право” в межах нової спеціальності 081 “Право” та програмою досліджень, яка має розкрити усі складові права національної безпеки у правовій системі України.

Водночас, поняття права національної безпеки, його ознаки та місце у системі права України продовжує мати досить проблем, важливих для наукових розробок та соціальної практики.

Метою статті є визначення природи правових відносин у сфері національної безпеки, особливостей суб’єктів та об’єктів таких відносин, правової природи джерел права національної безпеки, взаємозв’язків та взаємодії права національної безпеки з конституційним правом та з іншими галузями публічного права і, перш за все, з військовим правом.

Виклад основного матеріалу. Національна безпека у своєму онтологічному значенні характеризує певне уявлення людини про умови її життєдіяльності, про умови існування суспільства, держави і, водночас, постає осмисленою та цілеспрямованою діяльністю, яка спрямована на забезпечення сталого існування та розвитку людини, суспільства і держави. Онтологічний дуалізм, який проявляється у взаємозалежності безпеки людини і безпеки суспільства, підтверджується емпіричністю суспільних відносин, соціальних комунікацій, урегульованих певною сукупністю норм права. Саме за таких умов формується відповідна модель правового змісту національної безпеки.

Водночас, на онтологічному перетині національної безпеки і права виявляється, що національна безпека втрачає будь-який сенс без участі держави, а саме – визначених Конституцією і законодавством України державних інститутів, зокрема: РНБО України, Збройних Сил та інших військових формувань України, державних органів спеціального призначення з правоохоронними функціями, правоохоронних і розвідувальних органів та інших суб’єктів сектору безпеки і оборони. Саме державні інститути є активними рушійними чинниками забезпечення національної безпеки, через діяльність яких національна безпека набуває свого змістовного значення. Право утворює певний сутнісний простір національної безпеки, затверджуючи її форму та цивілізаційні ознаки, що містяться у нормах права, у правових спільностях, консолідованих на основі відповідного правового режиму.

Отже, концептуальне розуміння права національної безпеки полягає у розкритті онтологічного значення емпіричних вихідних безпекового стану людини, суспільства і держави, а також діяльності з метою досягнення такого стану та у сутнісному сприйнятті взаємозв’язку права і держави, що є вкрай важливим. Формування правового змісту національної безпеки і набуття національною безпекою певної правової форми відбуваються внаслідок складного когнітивного процесу.

Важливою є та обставина, що утворення громадянського суспільства, досягнення загального соціального стану безпеки, якою і є національна безпека, формування

правової цілісної спільності – права національної безпеки відбуваються в одній площині та в одних темпоральних координатах. На цьому шляху важливим виявляється урівноважити запити усіх соціальних суб’єктів стосовно безпечних умов існування, попередити можливі конфлікти та вирішити існуючі суперечності на основі загальнозначущих, універсальних нормативів і цінностей, які містить право.

Право об’єднує зусилля усіх соціальних суб’єктів навколо вирішення проблеми забезпечення національної безпеки і цей складний процес відбувається навіть за умов протистояння, але більш успішно – за умов єдності і розуміння необхідності підпорядкування визначених правом безпекових нормативів. У цьому, власне, вбачається важливе призначення права національної безпеки.

Проте консолідованість дій таких соціальних суб’єктів як суспільство (інститутів громадянського суспільства), держава (інститутів публічної влади) та людина (індивідуальних і колективних суб’єктів) є чи не ідеальною ситуацією, яка безумовно характеризується успішним вирішенням завдань національної безпеки.

Річ у тому, що ставлення держави, державних інститутів, громадянського суспільства, його інститутів до першості права у вирішенні проблеми національної безпеки не є однозначним. Держава, в особі конкретних державних органів та внаслідок реалізації ними своїх завдань і функцій, досить часто перебільшує можливості публічної влади, у тому числі щодо встановлення тих чи інших правил поведінки у сфері національної безпеки. Інститути громадянського суспільства і громадські організації для досягнення поставлених цілей також можуть діяти всупереч вимогам права і чинного законодавства. Ігнорування державними інститутами чи інститутами громадянського суспільства правових вимог з очевидною закономірністю призводить до виникнення певного соціального вакууму, де відчутним стає дефіцит права, а відтак, поставлене завдання щодо забезпечення національної безпеки загалом та у конкретних сферах не має перспектив для успішного вирішення. Такий стан може бути подоланий за рахунок наближення права і держави та визначення виключно правового змісту діяльності держави й інститутів громадянського суспільства за усіма напрямами забезпечення національної безпеки. За цих обставин право національної безпеки, як системна правова цілісність, набуває неабиякого значення.

Напрями забезпечення національної безпеки є багатовекторними, що пов’язується, насамперед, з розмаїттям соціального буття та різноманітністю запитів колективних соціальних акторів та особистостей у контексті забезпечення безпечних умов існування. Проте, варто погодитися з усталеною позицією стосовно визначальних напрямів, на яких ґрунтуються питання національної безпеки, – суверенітет, територіальна цілісність, конституційний лад, безпечні умови життєдіяльності. Ось чому першочергового значення набувають питання ефективного правового регулювання діяльності суб’єктів сектора безпеки і оборони на національному та міжнародному рівнях. Питання, що стосуються діяльності цих суб’єктів, є важливими у формуванні концепції права національної безпеки та визначення його ознак з декількох причин. Насамперед, йдеться про виокремлення таких суб’єктів права національної безпеки як держава і громадянське суспільство. Подібна постановка питання призводить до узагальнення, яке шкодить визначенню змісту правових комунікацій (правовідносин) саме через надмірний рівень узагальнення і певне абстрагування. Проте, без такого узагальненого підходу визначити сутність суб’єкта права як певного абсолюту неможливо [6, с. 37-38]. Для обґрунтування наукової позиції стосовно визначення держави суб’єктом права національної безпеки достатньо звернутися до доктринального вирішення проблеми суб’єктів конституційного права і, застосувавши найширші напрацювання у розрізі

конституційно-правових відносин [7, с. 22-23], ми дійдемо цілком вірного висновку про те, що держава та її органи, Збройні Сили та інші інститути сектору безпеки і оборони у межах визначеної законодавством компетенції та через належність до вказаного сектору, є суб’єктами права національної безпеки.

Іншою проблемою наукового пошуку щодо концептуальних засад права національної безпеки є визначення громадянського суспільства як суб’єкта цієї правової спільності. Тут також стикаємося із застосуванням узагальненого рівня юридичного пізнання, що у подальшому вимагатиме більшої конкретизації. Така конкретизація засновується на висновку про необхідність сформованості хоча б основ громадянського суспільства для утвердження самої ідеї національної безпеки. Сформоване громадянське суспільство утворює умови для розгортання відповідної суб’єктної складової права національної безпеки, що дозволяє вважати такими суб’єктами, власне, громадянське суспільство, а вже потім, закономірно, – інститути громадянського суспільства з визначенням їхнього правового статусу та компетенції. Немає потреби перебільшувати значення права у забезпеченні національної безпеки. Зрозуміло, що право містить нормативно-ціннісні показники, які у своїй цілісності дозволяють забезпечити стійкість сформованого за рахунок взаємодії суспільства і держави безпекового середовища, важливого для людини, громадянського суспільства і держави. Водночас, право утворює нормативи процедурного і матеріального характеру стосовно поведінки суб’єктів у сфері національної безпеки, визначає і затверджує загальносоціальні цінності, які підлягають правовій охороні та здійснює таку охорону.

При цьому, необхідно мати на увазі, що у сфері національної безпеки виникнення і реальне існування протиріч між громадянським суспільством і державою є питанням, яке постійно відкрите для дискусії та опрацювання. Невирішеність таких протиріч активує у більшості випадків руйнування основ національної безпеки. Саме тому актуалізується роль правових механізмів подолання та залагодження конфліктів і суперечностей між суспільними потребами та державними можливостями, забезпеченими відповідними владними механізмами. Такі правові механізми вимагають застосування ефективного контролю за діяльністю інститутів держави у сфері національної безпеки, які відносяться до сектору безпеки і оборони. Найбільш дієвим визнається демократичний цивільний контроль, у т.ч. контроль громадянського суспільства, який здійснюється відповідно до приписів права національної безпеки інститутами громадянського суспільства.

Отже, громадянське суспільство як суб’єкт права національної безпеки діє у сфері національної безпеки через відповідні інститути, взаємодіє з інститутами держави та бере участь у здійсненні демократичного контролю за діяльністю суб’єктів сектору безпеки і оборони.

Суб’єктний склад права національної безпеки визначає людину як найбільш важливого суб’єкта права, статус якого є повністю залежним від реалізації парадигми національної безпеки. Найголовніше право людського буття – право на життя фактично проголошує основну ідею національної безпеки у її антропологічному значенні. Інші найбільш важливі права людини підтверджують та розгортають властивості людини як суб’єкта права національної безпеки. Необхідно звернути особливу увагу на ту обставину, що процес онтологічного осмислення первинних емпіричних даних щодо безпечних умов людського буття повністю залежить від свідомого ставлення людини та її участі у подальшому формуванні, реалізації нормативно-ціннісних установок стосовно національної безпеки. Без усвідомлення людиною численних обставин, які становлять причини, умови, зміст соціального стану безпеки власного існування будь-які ідеї, а тим

більше дії, стосовно нормативно-ціннісного обґрунтування національної безпеки, яким і є право національної безпеки, втрачають онтологічний сенс і практичне значення. Натомість, важливого значення набуває суб’єктивне право людини на безпечні умови життєдіяльності, що змушує по-іншому розглядати реалізацію у праві національної безпеки відповідних конституційних положень, а саме – вихідних, основоположних ідей стосовно правового статусу людини і громадянина.

Право національної безпеки має власні об’єкти, визначення яких безпосередньо залежить від змісту національної безпеки. Як відомо, поширеною у юриспруденції є наукова позиція щодо дихотомії об’єктів права: під об’єктами права загалом розуміють матеріальні та нематеріальні блага, з приводу яких виникають та існують правові відносини, а також суспільні відносини (соціальні комунікації), правове регулювання або правове упорядкування яких здійснюють норми права. Звичайно, норми права мають своїм адресатом поведінку людей та поведінкові акти суб’єктів соціальних комунікацій. Норми права вказують на ціль, якої бажають і повинні досягти суб’єкти права. Цілеспрямування права визначає об’єкт його дії і у цьому діалектично поєднуються цінності та інтереси, набуваючи матеріальної або ж навпаки, нематеріальної, проте реальної форми.

Стверджуючи про матеріальні і нематеріальні блага, як об’єкти права національної безпеки, ми маємо на увазі матеріальні та нематеріальні характеристики безпеки, безпекового стану людського існування, що є не лише передумовою статусної природи людини, але й необхідною умовою фізичного існування усіх без винятку соціальних суб’єктів. Такий підхід демонструє найбільш широке розуміння об’єктів права національної безпеки. Але саме такий підхід дозволяє виокремити в усій її повноті сферу права національної безпеки, за межами якої перестають існувати ознаки людського буття, ознаки соціуму. Висловлена позиція не суперечить більш конкретному розумінню об’єктів права національної безпеки, якими є національні інтереси, потреби і цінності людського існування, прагнення людини у тій чи іншій галузі сфери національної безпеки – від державної, воєнної до інформаційної, техногенної тощо.

Національні інтереси визначають цілі та завдання не лише держави, але й суспільства в цілому. Юридизація національних інтересів полягає у їхньому законодавчому закріпленні та у правовій охороні. Через право національні інтереси набувають загальної значущості для суспільства, для індивідуальних і колективних суб’єктів. Національні інтереси відносяться до публічних інтересів і мають розглядатися як охоронювані законом інтереси. Такий висновок засновується на положеннях Конституції, як суспільного договору, який визначає основні та незмінні правила взаємовідносин між людиною і державою, між суспільством, його інститутами і державою, інституційними утвореннями держави. Національні інтереси, як об’єкти права національної безпеки, існують незалежно від суб’єктивних прав та юридичних обов’язків суб’єктів правовідносин сфери національної безпеки, проте об’єктивація національних інтересів є необхідною для формування суб’єктивних прав і юридичних обов’язків у конкретних правовідносинах вказаної сфери соціальних комунікацій.

Право національної безпеки, як і правовідносини у сфері національної безпеки, формується внаслідок дії правового режиму, який містить предмет – суспільні відносини між суб’єктами цієї сфери, метод – сукупність засобів і способів правового впливу (правового регулювання) на вказані суспільні відносини та мету, яка конкретизується відповідно до певної галузі соціального буття та певних безпечних умов життєдіяльності безпосередньо у сфері національної безпеки.

Правовий режим сфери національної безпеки характеризується досить жорсткими правилами упорядкування суспільних відносин, що забезпечує імперативний метод правового регулювання. Такий правовий режим може набувати спеціальних ознак надзвичайного режиму або ж режиму воєнного стану, що, зокрема, характеризує його виключну публічно-правову природу, зосереджену на охороні загальнозначущих інтересів. Зауважимо, що навіть за таких умов зберігається особливий порядок обмеження прав і свобод людини, проте жодним чином ці обмеження не можуть поширюватися на забезпечення і реалізацію права на безпечні умови людського існування. Домінування національних інтересів в об’єктивації права національної безпеки має межу, якою стає забезпечення права людини на життя, а інші основоположні права і свободи людини у виключних випадках обмежуються заради збереження життя людини і соціуму загалом.

Суспільні відносини (соціальні комунікації) у сфері національної безпеки мають різний зміст, проте об’єднує такі суспільні відносини під дією спеціального правового режиму загальна мета – забезпечення національної безпеки, що на практиці полягає у захисті національних інтересів від реальних і потенційних викликів та загроз. Мета правового регулювання суспільних відносин сфери національної безпеки, на чому необхідно наголосити, визначається відповідно до певних галузей соціального буття, суспільної діяльності – інформаційної, економічної, екологічної тощо. У такий спосіб формуються умови для задоволення запитів суб’єктів стосовно забезпечення національної безпеки, а також встановлюються відповідні правила діяльності суб’єктів у тій чи іншій сфері національної безпеки.

Захищеність національних інтересів, створення безпечних умов соціального буття виявляється цілісним та засвідчує правило, відповідно до якого необхідним є формування безпеки не лише на загальному рівні, але й у кожній сфері життєдіяльності людини, суспільства і держави. Загальна картина безпечних умов життєдіяльності залежить від такого стану у різних сферах національної безпеки, що регламентується нормами права національної безпеки. Зокрема, досягнення воєнної безпеки не гарантує національної безпеки за умов неспроможності протидіяти загрозам екологічного чи техногенного характеру. Загрози економічній безпеці, у разі неможливості їхнього подолання, також впливають на стан національної безпеки і потребують відповідної протидії. Відсутність спроможності досягти інформаційної безпеки утворює реальні й потенційні загрози воєнній та національній безпеці тощо.

Таким чином, єдність об’єктів права національної безпеки є необхідною з огляду на загальну мету, а конкретизація у відповідних галузях сфери національної безпеки є підтвердженням цілісності, що безумовно впливає на утворення цілісності права національної безпеки. Об’єкти права національної безпеки утворюють певні системні множинності національних інтересів – життєво важливих інтересів людини, суспільства і держави, реалізація яких забезпечує не лише суверенне існування держави, суспільства, а також людини в умовах суверенності держави, але й демократичний розвиток державної організації суспільства, безпечні умови життєдіяльності та добробут громадян. Формування права національної безпеки, як системної цілісної множинності норм права, має багато у чому нелінійний характер і залежить від об’єктивної соціальної необхідності нормативно-правового упорядкування суспільних відносин (соціальних комунікацій) для досягнення мети – безпечних умов існування та життєдіяльності людини, суспільства і держави. Норми і правила поведінки, що містить право національної безпеки, засновуються на суспільному договорі, яким є Конституція, і передбачають збереження не просто національної ідентичності, а досягнення

національної безпеки – стану, що засвідчує захищеність суверенітету, територіальної цілісності, конституційного ладу, тобто стану, який забезпечує сталий розвиток суспільства і держави. Відтак, право національної безпеки повною мірою використовує нормативні положення і приписи Конституції, конституційного права у контексті регулювання суспільних відносин щодо забезпечення національної безпеки.

На основі предмета і мети правового регулювання право національної безпеки консолідує відповідні нормативно-правові приписи інформаційного, адміністративного, екологічного, фінансового та інших галузей права, досягаючи того рівня комплексності, який дозволяє ефективно та успішно забезпечувати дію права у сфері національної безпеки.

При цьому виявляється, що найбільш стійкими є зв’язки права національної безпеки з військовим правом, де спільність об’єктів і суб’єктів, єдність правового режиму щодо забезпечення воєнної безпеки, захисту суверенітету і територіальної цілісності змушують поєднувати не лише наукові розробки, але й правозастосовну практику. Інституційна складова, функціональне призначення права національної безпеки і військового права є багато у чому спільними і такими, що взаємодоповнюють ці складові системи права.

Важливим у формуванні права національної безпеки, як галузі права, є використання власних юридичних джерел – нормативних приписів Конституції, законодавства, судових актів, доктринальних положень. Така ситуація, зрештою, змушує зосереджувати увагу на необхідності виокремлення в окрему галузь не лише законодавство про національну безпеку, але й відповідні наукові знання та практику застосовування, що звичайно, дозволяє стверджувати про окрему галузь юридичної науки і навчальної дисципліни, якими постає право національної безпеки. Також варто підтримати обґрунтовані пропозиції щодо формування наукової спеціалізації, яка передбачатиме проведення наукових розробок з проблем права національної безпеки і військового права [8, с. 66-68].

Особливого значення в сучасних умовах гібридної війни проти України набуває правове забезпечення національної безпеки. Зважаючи на особливості дії права у сфері національної безпеки, правове забезпечення національної безпеки можливо розглядати як важливу специфічну функцію права національної безпеки. Право національної безпеки, безумовно, виконує й інші функції стосовно своєї предметної сфери дії. Регулятивна, охоронна функції по-особливому реалізуються у праві національної безпеки, засвідчуючи його специфіку, як галузі права, та, віддзеркалюючи шляхи, способи, заходи, дії щодо забезпечення національної безпеки.

Право національної безпеки виконує превентивну функцію, попереджуючи настання загроз потенційного чи реального характеру для безпечних умов життєдіяльності. Очевидно, що більш значущими у цьому аспекті є нормативно-правове визначення і подолання потенційних загроз. Вказана функція доповнюється прогностичною функцією, яку виконує право національної безпеки у вирішенні завдань забезпечення безпекового стану існування людини, суспільства і держави.

Досить вагомою є інформаційна функція права національної безпеки, яка дозволяє не лише своєчасно і повно поширити у суспільстві інформацію про загрози національній безпеці, про заходи їх подолання, але й забезпечити надходження такої інформації спеціальним суб’єктам права національної безпеки, які мають виконувати завдання стосовно подолання, нейтралізації потенційних і реальних загроз національній безпеці.

Основоположним принципом права національної безпеки є принцип верховенства права, зміст якого доповнюється і конкретизується у принципі законності. Верховенство

права у сфері національної безпеки виявляється у визначенні та підпорядкуванні праву спрямованої на забезпечення національної безпеки діяльності усіх суб’єктів.

Правова поведінка у сфері національної безпеки стає переконливим аргументом для досягнення мети – стану безпеки суспільного життя, існування і функціонування індивідуальних та колективних суб’єктів. Принцип законності забезпечує реалізацію вимоги щодо інституціоналізації сфери національної безпеки та, насамперед, сектора безпеки і оборони, на підставі положень Конституції та чинного законодавства, визначення і реалізації функцій суб’єктів права національної безпеки виключно у відповідності до положень Конституції та прийнятих у її розвиток законів.

Принципом права національної безпеки також є відповідність його норм вимогам міжнародного права та міжнародних договорів, учасником яких є Україна. Важливим принципом права національної безпеки необхідно розглядати охорону і гарантування прав і свобод людини відповідно до вимог Конвенції про захист прав людини і основоположних свобод та практики ЄСПЛ. Попри первинність захисту і забезпечення прав і основоположних свобод людини у праві національної безпеки гармонійно поєднується цей принцип з принципом пріоритетності охорони загальнозначущих для суспільства і держави національних інтересів від потенційних і реальних загроз.

Висновки.

Проведене дослідження дозволяє обґрунтувати певні результати і зробити основні висновки, до яких необхідно віднести:

1) право національної безпеки є галуззю права – цілісною множинністю норм, тобто публічно визначених, легітимізованих правил поведінки, спрямованих на досягнення і забезпечення безпечних умов існування та життєдіяльності людини, суспільства і держави;

2) право національної безпеки у системі права України формується внаслідок дії правового режиму, маючи власний предмет, яким є суспільні відносини сфери національної безпеки, використовуючи метод, який полягає в імперативному впливі на поведінку учасників таких суспільних відносин і мету, якою постає стан безпеки, тобто захищеності національних інтересів від реальних і потенційних викликів та загроз;

3) суб’єктами права національної безпеки є людина, громадянське суспільство (інститути громадянського суспільства), держава (державні інститути); об’єкти права національної безпеки утворюють національні інтереси, які конкретизуються у різних галузях національної безпеки;

4) право національної безпеки виконує визначені у правовій системі України функції та засноване на принципах, які підтверджують його особливі ознаки та належність до системи права України як системної цілісності;

5) для права національної безпеки України властивим є поєднання лінійних і нелінійних характеристик, які обґрунтовують його утворення і функціонування як відокремленого комплексного компонента системи права;

6) джерелами права національної безпеки є Конституція, законодавство, судова практика та відповідні доктринальні положення, що стосуються правотворчості та правозастосування у сфері національної безпеки;

7) законодавство про національну безпеку утворює самостійну галузь у системі законодавства України;

8) право національної безпеки необхідно розглядати як галузь юридичної науки у межах наукової спеціальності 081 – “Право” та як окрему навчальну дисципліну;

9) найбільш стійкими у системі права є взаємозв’язки права національної безпеки з військовим правом, що дозволяє інтегрувати інституційну та функціональну складові

цих системних комплексних утворень на рівні нормативно-правового регулювання, правозастосовної практики та подальших наукових досліджень.

Використана література

1. Пилипчук В.Г. Пріоритети розвитку правової науки в галузі національної безпеки / Стратегічна панорама. – К. : НІСД. – 2009. – № 2. – С. 36-40.

2. Горбулін В.П. Національна безпека як пріоритет сучасного державотворення // Вісник Національної академії наук України. – 2017. – № 1. – С. 25-29.

3. Власюк О.С. Національна безпека України : еволюція проблем внутрішньої політики / О.С. Власюк. – (Вибр. наук. праці). – К. : НІСД, 2016. – 528 с.

4. Про рішення Ради національної безпеки і оборони України від 26 травня 2015 року “Про Стратегію національної безпеки України” : Указ Президента України від 06.05.15 р. № 287/2015. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/287/2015

5. Moore John Norton. National Security Law. Syllabus and Assighments. Spring 2017. URL: http://faculty.virginia.edu/jnmoore/pdf. – (Moore-National-Sec-Law -Vol- 01S.pdf Moore John Norton National Security Law & Police. Third Edition / John Norton Moore, Guy B. Roberts, Robert F. Turner, etc. – Durham, Carolina Academic Press, 2015 – 1608 p.).

6. Хаустова М. Суб’єкт права як елемент правової системи суспільства // Вісник Академії правових наук України. – 2009. – № 3. – С. 29-38.

7. Шаповал В. Суб’єкти конституційного права України : постановка проблем теоретичного визначення // Право України. – 2000. – № 8. – С. 21-24.

8. Пилипчук В.Г., Доронін І.М. Право національної безпеки та військове право: теоретичні та прикладні засади становлення і розвитку в Україні // Інформація і право. – 2018. – № 2. – С. 62-68.

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

УДК 658:330.87

ДОВГАНЬ О.Д., *доктор юридичних наук, старший науковий співробітник,*
НДІ інформатики і права НАПрН України
ТАРАСЮК А.В., *кандидат юридичних наук,* Служба безпеки України

ГЛОБАЛЬНА КУЛЬТУРА КІБЕРБЕЗПЕКИ В СИСТЕМІ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ

Анотація. *В статті досліджується питання дефініції поняття “глобальна культура кібербезпеки”, розглядаються принципи та підходи формування глобальної культури кібербезпеки на національному рівні. Основна увага приділяється складовим феномена культури кібербезпеки, її ролі та місцю в системі запобігання кіберзлочинності.*

Ключові слова: *кібербезпека, кіберзлочинність, протидія кіберзлочинності, система запобігання кіберзлочинності, глобальна культура кібербезпеки.*

Summary. *The article explores a definition of concept “global culture of cyber security”, the principles and approaches of forming a global culture of cyber security on the national level. The main focus is on the cyber security culture, its role and place in the system of cyber crime prevention.*

Keywords: *cyber security, cyber crime, countereffort of cyber crime, cyber crime prevention system, global cyber security culture.*

Аннотация. *В статье исследуется вопрос дефиниции понятия “глобальная культура кибербезопасности”, рассматриваются принципы и подходы формирования глобальной культуры кибербезопасности на национальном уровне. Основное внимание уделяется составляющим феномена культуры кибербезопасности, ее роли и месту в системе предупреждения киберпреступности.*

Ключевые слова: *кибербезопасность, киберпреступность, противодействие киберпреступности, система предупреждения киберпреступности, глобальная культура кибербезопасности.*

Постановка проблеми. Проблема протидії кіберзлочинності є одним із пріоритетів у системних заходах забезпечення кібербезпеки на національному та міжнародному рівні, має правовий, технічний і організаційний аспект у запобіганні, виявленні (розслідуванні), припиненні та розкритті кіберзлочинів. При цьому, складність, відповідно, і ефективність заходів виявлення, припинення та розкриття кіберзлочинів обумовлена технологічними особливостями процесів створення, зберігання, обміну, обробки та знищення інформації у сучасних технологіях кіберпростору, складністю доведення причетності конкретної особи до здійснення певних дій, юридичними особливостями надання офіційної правової допомоги від держав, з територіальної частини кіберпростору яких здійснювались кіберзлочини. В свою чергу, ефективність заходів запобігання кіберзлочинам визначається рівнем достатності заходів стримування потенційних правопорушників (зниженням ризику вчинення кіберзлочинів), можливостями усунення або зменшення потенційно шкідливих наслідків вчинення кіберзлочинів, а також організаційно-технічними характеристиками рівня захищеності всіх об’єктів кібербезпеки.

Загалом, протидія кіберзлочинності реалізується через систему заходів, спрямованих на усунення причин і умов, які сприяють вчиненню кіберзлочинів, які вже мають місце, або готуються чи вже почалися, виявлення винних осіб та притягнення їх до відповідальності. Разом з тим, ефективність заходів протидії кіберзлочинності визначається не лише ефективністю діяльності правоохоронних органів, а і ефективністю

діяльності національної і міжнародної системи кібербезпеки в цілому, включаючи і ефективність співпраці їх суб’єктів на національному і міжнародному рівнях.

Актуальність дослідження зумовлена сучасними викликами і загрозами проявів кіберзлочинності в Україні, необхідністю реалізації системних заходів протидії у рамках Національної системи кібербезпеки, національною відповідальністю за підтримання міжнародного правопорядку тощо.

Результати аналізу наукових публікацій. Проведений контентний аналіз публікацій В. Брижка, В. Бутузова, В. Гавловського, О. Довганя, М. Карчевського, В. Кудінова, М. Кравцової, В. Маркова, А. Марущака, О. Орлова, В. Пилипчука, Е. Рижкова, К. Тітуніної, В. Хахановського, В. Шеломенцева, О. Юрченка та інших авторів свідчать про достатню розробленість проблеми протидії кіберзлочинності, однак залишається малодослідженим соціальний аспект заходів запобігання кіберзлочинів, що стосується формування глобальної культури кібербезпеки.

Мета статті полягає у науковому обґрунтуванні сутності поняття “глобальна культура кібербезпеки”, основних складових, принципів та підходів до її формування. Завданнями статті є розкриття сутності феномена глобальної культури кібербезпеки через такі складові, як “кіберзлочинність”, “протидія та запобігання кіберзлочинності”, “культура та глобальна культура”, “професійна культура”, “культура кібербезпеки” та ін.

Виклад основного матеріалу. У науковій спільноті України ще має місце дискусія відносно визначення термінів у сфері кібербезпеки [1]. Однак, при проведенні дослідження будемо користуватися термінами “кібербезпека”, “кіберпростір”, “кіберзлочин”, “кіберзлочинність”, “кібершпигунство”, “кібертероризм”, “кіберзахист”, “кіберінцидент” та “кібератака” у відповідності з визначеннями, що запропоновані в Законі України “Про основні засади забезпечення кібербезпеки України”.

Формування та реалізація державної політики щодо запобігання та протидії кіберзлочинності – це процеси, що відбуваються в рамках Національної системи кібербезпеки, які можна розглянути через організаційно-правовий, організаційно-технічний та правоохоронний аспекти.

У рамках міжнародної співпраці Україною ратифіковано Конвенцію Ради Європи про кіберзлочинність, Угоду про асоціацію між Україною та Європейським Союзом, у якій передбачено, що сторони Угоди співробітничають, у тому числі, і з питань протидії кіберзлочинності. Крім того, одним із пріоритетів співпраці України з НАТО та США є співпраця в галузі протидії кіберзлочинності, в рамках якої Україна отримує можливість координації дій та обміну інформацією при розслідуванні кіберзлочинів.

На сьогодні Стратегія кібербезпеки України (рішення Ради національної безпеки і оборони України від 27 січня 2016 року), Указ Президента України “Про загрози кібербезпеці держави та невідкладні заходи з їх реалізації” (рішення Ради національної безпеки і оборони України від 29 грудня 2016 року) та Закон України від 05 жовтня 2017 року “Про основні засади забезпечення кібербезпеки України”, визначають організаційно-правову основу протидії кіберзлочинності, яка полягає, насамперед, у визначенні суб’єктів, сфер їх компетенції, напрямів взаємодії у рамках Національної системи кібербезпеки та міжнародної співпраці.

Так, у сфері компетентності Держспецзв’язку України, до організаційно-правових заходів запобігання і протидії кіберзлочинності відноситься регуляторна діяльність у сферах технічного і криптографічного захисту інформації, яка полягає у створенні умов для формування ринку засобів і послуг із захисту інформації у кіберпросторі *(забезпеченні конфіденційності, цілісності, підтвердження авторства та доступності інформації)*, а також забезпеченні необхідних рівнів кіберзахисту засобами і послугами,

що пропонуються як для юридичних, так і фізичних осіб. Тобто, мова йде про створення умов для забезпечення доступності надійних засобів і систем кіберзахисту для фізичних і юридичних осіб України.

Нормативно-правове забезпечення у сферах технічного і криптографічного захисту інформації:

– структурує та упорядковує відносини між державою, тими хто забезпечує та отримує захист інформації, насамперед, шляхом регулювання технічних регламентів із захисту інформації, що мають примусовий і рекомендаційний характер;

– стосується процедур ліцензування, розроблення, виготовлення, модернізації, експертизи, впровадження, експлуатації та виведення із експлуатації засобів і систем захисту інформації.

Серед чинних нормативно-правових актів виділимо: Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” від 19.04.2014 року; постанову Кабінету Міністрів України “Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” від 07.09.2011 року № 373; нормативний документ системи технічного захисту інформації “Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі” від 08.11.2005 року НД ТЗІ 3.7-003-05; нормативний документ системи технічного захисту інформації “Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу” від 20.12.2000 року НД ТЗІ 3.6-001-2000; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації” від 30.05.2007 року № 141; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про державну експертизу в сфері технічного захисту інформації” від 16.05.2007 року № 93; Наказ Адміністрації Держспецзв’язку України “Про затвердження Положення про державну експертизу в сфері криптографічного захисту інформації” від 23.06.2008 року № 100.

З метою забезпечення системності заходів протидії кіберзлочинності в Україні є актуальним завдання приведення до єдиних формулювань законодавство у сферах забезпечення кібербезпеки, технічного і криптографічного захисту інформації, визначення норм для віднесення об’єктів до критичної інформаційної інфраструктури тощо.

Організаційно-технічна складова заходів протидії кіберзлочинності полягає у впровадженні організаційно-технічної моделі кіберзахисту, включаючи забезпечення державно-приватної взаємодії при реалізації заходів запобігання, виявлення, реагування на кіберінциденти і кібератаки, усунення їх наслідків.

На сьогодні організаційно-технічна модель кіберзахисту доопрацьовується за участю компетентних вітчизняних структур та міжнародних експертів. При цьому, вона напевне повинна орієнтуватись на сучасні міжнародні практики, що базуються на ризик-орієнтованих стандартах управління кібербезпекою (сімейства стандартів з управління інформаційною безпекою ISO/IEC 270k), насамперед, ISO/IEC 27032 Guidelines for cybersecurity *(“Рекомендації з кібербезпеки”)*, а також ISO/IEC 27037 Guidelines for identification, collection, acquisition and preservation of digital evidence *(“Рекомендації щодо ідентифікування, збору, накопичення та збереження цифрових доказів”)*, ISO/IEC 27041 Guidance on assuring suitability and adequacy of incident investigative method *(“Настанова щодо забезпечення прийнятності та адекватності методів розслідування”)*, ISO/IEC 27043 Incident investigation principles and processes *(“Принципи та процеси розслідування інцидентів”)*. Загалом же організаційно-технічна модель

кіберзахисту повинна включати моделі оцінки ризику та прийняття рішень, а їх стандартизація та впровадження безпосередньо вплине на ефективність правоохоронних заходів із протидії кіберзлочинів в Україні.

Урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA [2] (Державний центр кіберзахисту) є акредитованим членом FIRST та активно взаємодіє з аналогічними командами в усьому світі, орієнтована на кіберзахист державних інформаційних ресурсів, співпрацює та допомагає правоохоронним, банківським, комерційним, іншим державним і приватним структурам. Однак, цього недостатньо, провідні країни світу мають більше 20 CERT, у тому числі і в правоохоронних органах, інших суб’єктах Національної системи кібербезпеки і у вищих навчальних закладах зокрема.

Правоохоронний аспект в системі протидії кіберзлочинності стосується передусім кримінальної відповідальності для осіб, що вчинили кіберзлочини. Так, у відповідності з КК України розслідуються наступні категорії злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж [3]: ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку); ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут); ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації); ст. 362 (Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї), ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється); ст. 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку).

Крім цього [3], варто звернути увагу на: ст. 176 *(Порушення авторського права і суміжних прав)*; ст. 185 *(Крадіжка)*; ч. 3, 4 ст. 190 *(Шахрайство)*; ст. 200 *(Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення)*; ст. 229 *(Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару)*; ст. 231 *(Незаконне збирання інформації, що становить банківську таємницю)*; ч. 3 – 5 ст. 301 *(Ввезення, виготовлення, збут і розповсюдження порнографічних предметів)*.

Виходячи із сучасних уявлень про кібербезпеку, неможливо оминути увагою також кримінальні правопорушення з використанням можливостей соціальних мереж (кіберпростору), відповідальність за вчинення яких передбачено такими статтями КК України [4]: ст. 120 *(Доведення до самогубства)*; ст. 160 *(Підкуп виборця, учасника референдуму)*; ст. 161 *(Порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за ін. ознаками)*; ст. 163 *(Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв’язку або через комп’ютер)*; ст. 189 *(Вимагання)*; ст. 192 *(Заподіяння майнової шкоди шляхом обману або зловживання довірою)*; ст. 258-4 *(Сприяння вчиненню терористичного акту);* ст. 258-2 *(Публічні заклики*

до вчинення терористичного акту); ст. 338 *(Наруга над державними символами)*; ст. 345-1 *(Погроза або насильство щодо журналіста)*; ст. 350 *(Погроза або насильство щодо службової особи чи громадянина, який виконує громадський обов’язок)* та ін.

У свою чергу, ратифікована Україною Конвенція Ради Європи про кіберзлочинність визначає: правопорушення проти конфіденційності; правопорушення, пов’язані з комп’ютерами (проти цілісності та доступності інформації); правопорушення пов’язані зі змістом; правопорушення пов’язані з порушенням авторських та суміжних прав.

Сьогоднішня практика кіберполіції пропонує громадянам звертатись [5]: щоб повідомити інформацію про суїцидальні групи в Інтернет; якщо є інформація про ресурси чи осіб, що поширюють порнографію, порушують авторські чи суміжні права в Інтернет; якщо є дані про торгівлю наркотиками чи зброєю, або інші види забороненої в мережі інтернет діяльності; щоб повідомити про матеріали, які закликають до сепаратизму чи тероризму; для надання інформації щодо спроб незаконного зняття коштів з рахунків; викрадення даних платіжних карток чи інших фінансових шахрайств, зокрема, про фінансові піраміди в Інтернеті, про скімінг, кардерство тощо; щоб повідомити про віруси, ботнети чи інші види інтернет шахрайства. Фактично, охоплює всі напрями протидії кіберзлочинності, що віднесені до підслідності органів внутрішніх справ. Але, у Національній системі кібербезпеки є також актуальними питання щодо ефективної протидії правопорушенням у кіберпросторі, які стосуються боротьби зі спамом, захисту персональних даних, комерційної таємниці та ін.

Отже, здається очевидним завдання приведення до єдиних формулювань диспозиції та кваліфікуючих ознак КК України, що передбачають відповідальність за злочини, які можна віднести до категорії кіберзлочинів.

За результатами аналізу статистичної інформації щодо протидії кіберзлочинності можна стверджувати, що практика припинення і розкриття кіберзлочинів стикається зі значними труднощами, зумовленими складністю виявлення цих високотехнологічних злочинів, високим рівнем їх латентності. Тому розглядаються криміналістичні характеристики кіберзлочинів [6]: типові слідчі ситуації; спосіб вчинення та приховання злочину; типові матеріальні сліди злочину та механізм слідоутворення; характеристика особистості обвинуваченого й потерпілого; обстановка злочину. Водночас, широкий спектр ІТ-технологій, що використовуються правопорушниками, передбачають анонімність та захищеність у кіберпросторі, відповідно, відзначаються різноманітністю та складністю механізмів слідоутворення з можливістю приховання або змін комп’ютерної/мережевої інформації щодо слідів злочину. Зазначені чинники не сприяють чіткому уявленню щодо всіх компонентів криміналістичної характеристики кіберзлочинів, а в кінцевому підсумку, ускладнюють процес розкриття кіберзлочинів відповідно [6].

Тому є актуальною потреба у постійному удосконаленні тактики проведення слідчих дій із розслідування кіберзлочинів, методик та ефективних методів комп’ютерно-технічної експертизи, що відповідають сучасним реаліям та тенденціям розвитку ІТ-технологій.

Далі, під системою протидії кіберзлочинності у широкому розумінні (не обмежуючись правоохоронною діяльністю) можна розуміти взаємопов’язану сукупність організаційно-правових, організаційно-технічних та правоохоронних (кримінологічних і криміналістичних) заходів запобігання, виявлення, припинення та розкриття кіберзлочинів.

У свою чергу, під системою запобігання кіберзлочинності можна розуміти сукупність взаємопов’язаних спеціально-кримінологічних, індивідуальних та загальних

заходів попередження, спрямованих на виявлення й усунення причин та умов, які сприяють вчиненню кіберзлочинів.

Спеціальне попередження кіберзлочинів здійснюється в рамках правоохоронної діяльності шляхом впливу на соціальні групи, окремих осіб і організації щодо яких є підстави вважати, що вони мають підвищену криміногенність. Суб’єктом індивідуального попередження як одного із видів спеціального попередження, є конкретна людина, особисті характеристики якої об’єктивно говорять про можливість здійснення нею у майбутньому злочинного діяння. Спеціальне попередження повинно передбачати заходи формування та ведення оперативних і профілактичних обліків визначених груп суб’єктів підвищеного кіберкриміногенного ризику, активізацію превентивної діяльності щодо виявлення осіб, схильних до вчинення кіберзлочинів, запобігання й припинення їх кримінальної активності тощо [7].

Загальне попередження кіберзлочинів:

– являє собою системні соціальні заходи державних органів Національної системи кібербезпеки, громадських організацій та бізнесу, які спрямовані на зниження ризику вчинення кіберзлочинів, усунення або зменшення потенційно шкідливих наслідків від їх вчинення;

– реалізується шляхом управління кібербезпекою на корпоративному рівні, забезпеченням широких верст населення надійними засобами і послугами із кіберзахисту, формуванням обізнаності суспільства в питаннях кіберзахисту, що стосуються, насамперед, організаційно-технічних та правоохоронних аспектів;

– орієнтоване на категорію потенційних потерпілих від кіберзлочинів, які не є фахівцями з ІТ-технологій та кіберзахисту, має за мету зменшення їх уразливості за рахунок формування глобальної культури кібербезпеки.

Відтак, узагальнюючи результати проведеного дослідження маємо всі підстави для твердження, що в сучасних умовах розвитку та впровадження ІТ-технологій в Україні, заходи формування культури кібербезпеки є доволі ефективним механізмом протидії кіберзлочинності. І, звісно, мова йде про системні заходи забезпечення кібербезпеки у розрізі небезпек життєво важливим інтересам особистості у кіберпросторі, з позицій захисту інформації та інформаційно-психологічного захисту (захисту від інформації) відповідно.

Глобальна культура кібербезпеки – це шлях вирішення проблеми підвищення рівня кіберзахисту особи і суспільства з використанням соціальних заходів на міжнародному і національному рівнях. Актуальність цієї проблеми обумовлена наявними і прогнозованими тенденціями збільшення кількості кримінальних правопорушень у кіберпросторі у зв’язку зі значним поширенням технологій електронної економіки та урядування, безпрецедентними масштабами комунікації у кіберпросторі спільнот національного і міжнародного виміру.

Історично, термін “культура кібербезпеки” був використаний саме у глобальному розумінні в Резолюції Генеральної Асамблеї “Створення глобальної культури кібербезпеки” (Creation of a global culture of cybersecurity) у 2002, 2003 та 2009 роках, хоча у цих документах не запропоновано його визначення. Зазначені документи були запропоновані як рекомендації для розроблення національних стратегій кібербезпеки, що визначають сутність національних систем кібербезпеки та заходи з поширення передових практик кіберзахисту.

Досліджуючи дефініцію “глобальна культура кібербезпеки” доцільно, перш за все, звернути увагу на концепти масової та глобальної культури. Так, спираючись на поняття кібербезпеки і кіберпростору, під “масовістю” будемо розуміти обсяг носіїв культури,

фактично, широкі верстви населення – масового користувача. В свою чергу, під “глобальністю” розуміємо не інтеграцію національних культур, а феномен наднаціональної професійної культури. Тобто, глобальну культуру кібербезпеки можна розглядати як наднаціональну масову культуру кібербезпеки, що охоплює категорії “культури кібербезпеки”, “інформаційної культури”, “професійної культури”, “культури” тощо.

Очевидно, що дослідження проблеми формування глобальної культури кібербезпеки має міждисциплінарний характер та потребує розгляду з позицій філософії, культурології та соціології.

Термін “культура” походить від латинських слів: “colo”, що означає “обробіток”; “colore” – “обробляти, вирощувати”, а пізніше – “поклонятися та вшановувати богів та предків”; “cultura”, що означає “обробіток, виховання, освіту” – систему надбіологічних програм людської діяльності, поведінки, спілкування, які історично еволюціонують. У сучасному розумінні культура – це складний суспільний феномен життєдіяльності людини, що стосується побуту, дозвілля, способу життя як окремої особи, так й усього суспільства.

У філософії культура (матеріальна і духовна категорія) розглядається у всесторонньому історичному розумінні як: процес розвитку людських сил і здібностей; показник міри людського в людині; характеристика розвитку людини як людської істоти; процес освоєння природи, який одержує своє зовнішнє вираження у всьому багатстві і різноманітті створюваної людьми дійсності, у всій сукупності результатів людської праці і думки. При цьому, на думку більшості сучасних філософів, в структурі феномена культури можна виділити два класи елементів. Перший характеризує культуру як систему еталонів суспільної поведінки людей, другий – як систему, що здійснює соціальний контроль над цінностями та ідеями. Вочевидь, у контексті запобігання кіберзлочинності доцільно розглядати матеріальну культуру в розумінні системи еталонів суспільної поведінки людей.

В даний час у культурології виділяють передусім наступні аспекти культури як неприродного штучного явища:

– генетичні – культура є продуктом суспільства з позиції її виникнення;

– гносеологічні – культура є сукупністю досягнутих у процесі освоєння світу матеріальних і духовних цінностей;

– гуманістичні – культура є розвитком самої людини, її духовних, творчих здібностей;

– психологічні – культура є процесом адаптації до життєвого середовища, навчання та формування звичаїв;

– історичні – культура є процесом соціального наслідування та формування традицій;

– структурні – культура є організованими повторювальними реакціями суспільства звичаями та традиціями;

– правові – культура є системою, що регулює соціальні відносини в суспільстві, орієнтує людину в світі;

– соціологічні – культура є обмеженнями в діяльності конкретного соціального суб’єкта, а також станом і розвитком тієї чи іншої діяльності.

Загалом, у соціології культура вважається життєвим устроєм суспільства (мова, звичаї, символи і об’єкти матеріальної культури) та результат соціальної взаємодії:

– щодо створення, засвоєння, збереження та розповсюдження предметів, ідей, ціннісних уявлень, які забезпечують взаєморозуміння людей в різних соціальних ситуаціях;

– соціальних суб’єктів з життєвим середовищем, який забезпечує формування досвіду, розвиток форм та способів діяльності.

При цьому, соціологія культури – це спеціальна соціологічна теорія, яка вивчає закономірності функціонування культури в суспільстві через приму трьох основних складових: ставлення людей до природи; ставлення до інших людей; ставлення людини до самої себе (самопізнання, самовиховання, самовдосконалення, саморозвиток).

У загальному випадку Вікіпедія пропонує розуміти під культурою сукупність матеріальних та духовних цінностей, створених людством протягом його історії; історично набутий набір правил всередині соціуму для його збереження та гармонізації. Серед видів культури – культуру суспільства, організації та особистості.

Отже, виходячи із завдань запобігання кіберзлочинності варто звернути увагу на психологічний, правовий та соціологічний аспекти культури суспільства, особистості соціальної взаємодії з формування досвіду, розвитку форм та способів інформаційній діяльності у кіберпросторі.

Далі розглянемо таку категорію як “професійна культура” і її складові – “правову, управлінську та інформаційну культуру”, “культуру кібербезпеки” відповідно. В науковому середовищі запропоновано багато визначень професійної культури як специфічної культури професійного товариства та його представників, зокрема, з позицій аксіологічного, діяльнісного та особистісного підходів під професійною культурою можна розуміти [8]:

– систему професійних цінностей, професійних норм і переконань, професійних традицій, що обумовлюють ставлення фахівців до предметів і об’єктів їх діяльності;

– єдність професійної зрілості, професійної етики, естетики, громадянської й етичної вихованості;

– характеристика рівня і якості професійної діяльності, яка залежить від соціально-економічного стану суспільства й сумлінності в оволодінні певними знаннями, навичками конкретної професії та їх практичному використанні;

– інтегральний показник діяльності, що забезпечується єдністю та взаємодією всіх її чинників, включаючи тезаурус і кругозір, вміння і здібності, діапазон інтересів, світогляд, норми і методи діяльності, культуру почуттів тощо.

При цьому, загальновідомо, що правова культура – це система правових цінностей, що відповідають рівню досягнутого суспільством правового процесу і відбивають у правовій формі стан свободи особи та інші соціальні цінності. Культура управління являє собою культурологічний підхід до змісту, видів, функцій та методів управління, стосується процесу управління, спирається на мораль, етику, естетику та особливості професійної діяльності. Інформаційна культура у вузькому розумінні ототожнюється з поняттям цифрової грамотності (компетентності – знання, вміння і навички, особистісні якості суб’єктів інформаційної діяльності), яка необхідна для ефективної інформаційної діяльності.

Інформаційна культура передбачає також [9] високий рівень загальної культури міжособистісного спілкування; готовність толерантно сприймати іншу точку зору; вміння аргументовано вести дискусії, готовність визнати себе переможеним у цій дискусії; готовність не тільки отримувати нові знання, а й ділитися своїми; знання норм і правил, що регламентують використання інтелектуальної власності і готовність користуватися ними тощо.

Виходячи із мети та завдань статті, зосередимо увагу на наступних аспектах професійної культури: етичних нормах інформаційної діяльності, компетентності; змісті, видах, та методах професійного переконання суспільства щодо необхідності виконання етичних норм та технічних регламентів безпеки, формуванні професійної зрілості широких верств населення з питань кібербезпеки.

Крім того, звернемо також увагу на визначення культури кібербезпеки у звіті 2017 року Європейського агентства з питань мережевої та інформаційної безпеки (ENISA) “Культура кібербезпеки організації” [10]: знання, переконання, уявлення, норми і цінності людей по відношенню до кібербезпеки та використанню інформаційних технологій.

Таким чином, спираючись на отримані результати дослідження щодо запобігання кіберзлочинності та сутності професійної культури, під “культурою кібербезпеки” будемо розуміти систему переконань, уявлень та етичних норм щодо ведення інформаційної діяльності у кіберпросторі, знань, вмінь та навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності у кіберпросторі.

У свою чергу, “глобальною культурою кібербезпеки” будемо вважати наднаціональну масову культуру кібербезпеки суспільства, організацій та особистості.

При цьому, основною метою формування глобальної культури кібербезпеки є досягнення такого стану соціальної взаємодії між суб’єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів кіберпростору.

Далі зазначимо, що у Резолюції Генеральної Асамблеї ООН було запропоновано дев’ять взаємопов’язаних принципів глобальної культури кібербезпеки: *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що вони можуть здійснити для підвищення безпеки); *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі); *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявленню та реагуванню, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективне співробітництво з попередження, виявлення та реагування на такі інциденти); *етика* (врахування законних інтересів інших); *демократія* (безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність); *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього, з урахуванням значущості інформації, яка захищається); *проектування та впровадження засобів забезпечення безпеки; переоцінка* (належні та своєчасні заходи з внесення змін у політику, практику забезпечення безпеки з урахуванням нових та зміни існуючих загроз)

Світова практика формування глобальної культури кібербезпеки та реалізації зазначених принципів базується на рекомендаціях міжнародних організацій та національних ініціативах, насамперед, шляхом: інформування (формуванням обізнаності) широких верств населення, фахівців державних і приватних установ відносно існуючих загроз, заходів попередження їх реалізації, виявлення та реагування; формування та підтримки ринку засобів та послуг кіберзахисту, проведення відповідного навчання. Національні стратегії кібербезпеки передбачають механізми взаємодії та відповідальності в рамках приватно-державного партнерства при реалізації заходів формування глобальної культури кібербезпеки.

Заходи формування обізнаності громадян з питань забезпечення кібербезпеки відбуваються шляхом інформування співробітників організацій та установ різних форм власності: в засобах масової інформації; на веб-ресурсах державних і приватних структур; на конференціях, семінарах та тренінгах; при реалізації освітніх програм в середніх і вищих навчальних закладах. Формування та підтримка ринку засобів і послуг із забезпечення

кібербезпеки передбачає: заходи нормативно-правового регулювання сфери технічного і криптографічного захисту інформації; створення громадських організацій для надання правової і технічної допомоги громадянам для забезпечення їх кібербезпеки; розбудову національної системи оповіщення про кібератаки та кіберінциденти; започаткування механізмів страхування ризиків та інших інструментів управління кібербезпекою.

Висновки.

Формування глобальної культури кібербезпеки є дієвим механізмом запобігання кіберзлочинності, який спрямовано на попередження, виявлення й усунення причин та умов, які сприяють вчиненню кіберзлочинів. Мова йде про системні заходи забезпечення життєво важливих інтересів осіб у кіберпросторі, з позицій захисту інформації та інформаційно-психологічного захисту.

В сучасних умовах державна політика з питань формування глобальної культури кібербезпеки повинна бути спрямована на ефективну координацію діяльності правоохоронних органів, державних і бізнес структур, інститутів громадянського суспільства, мати за мету подолання цифрової нерівності та забезпечення доступності правових і технічних механізмів захисту особи у кіберпросторі.

Перспективою подальших досліджень є нормативно-правові та організаційні аспекти формування глобальної культури кібербезпеки на національному та міжнародному рівні.

Використана література

1. Довгань О.Д. Ескалація кіберзагроз національним інтересам України та правові аспекти кіберзахисту : монографія / О.Д. Довгань, І.М. Доронін. – (НДІ інформатики і права НАПрН України – К. : Видавничий дім “АртЕк”. – 2017. – 107с.

2. CERT-UA. – Режим доступу : https://cert.gov.ua

3. Марущак А.І. Інформаційно-правові аспекти протидії кіберзлочинності // Інформація і право. – 2018. – № 1(24). – С. 127-132.

4. Гавловський В.Д. Кримінологічний аналіз злочинів, учинених з використанням соціальних мереж // Інформація і право. – 2017. – № 3(22). – С. 101-107.

5. Кіберполіція Києва. – Режим доступу : https://kyivcity.gov.ua/bezpeka_ta_pravoporiadok/kyivska_politsiia/kiberpolitsiia_kyieva.html

6. Серьогін В.С., Леонов Б.Д. Окремі проблеми криміналістичного забезпечення розслідування злочинів, пов’язаних з неправомірним дистанційним доступом до комп’ютерної інформації // Інформація і право. – 2017. – № 2(21). – С. 108-115.

7. Кравцова М.О. Кіберзлочинність : кримінологічна характеристика та запобігання органами внутрішніх справ : автореф дис. на здобуття наук. ступеня к.ю.н. : 12.00.08 / М.О. Кравцова. – (Харківський університет внутрішніх справ). – Харків, 2016. – С. 19.

8. Миколаєнко Н.М. Сутнісна характеристика поняття “професійна культура” / Естетичне виховання дітей та молоді : теорія, практика, перспективи розвитку : зб. наукових праць ; за ред. О.А. Дубасенюк, Н.Г. Сидорчук. – Житомир : Вид-во ЖДУ ім. І. Франка, 2012. – С. 539-545.

9. Довгань О.Д. Щодо деяких правових аспектів культури кібербезпеки: зб. тез наукових доповідей IX Всеукраїнської науково-практичної конференції [“Актуальні проблеми управління інформаційною безпекою держави”]. – К., 2018. – Ст. 60-62.

10. Report The European Union Agency for Network and Information Security (ENISA) Cyber Security Culture in organisations. URL: //https://www.enisa.europa.eu/publications/ cyber-security-culture-in-organisations

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

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

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У БОРОТЬБІ З ТРАНСНАЦІОНАЛЬНОЮ КІБЕРЗЛОЧИННІСТЮ

Анотація. *У статті досліджуються питання міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю. Сформульовано пропозиції щодо покращення співробітництва вітчизняних правоохоронних органів із зарубіжними партнерами з метою підвищення оперативності розслідування відповідних злочинів.*

Ключові слова*: міжнародне співробітництво, кіберзлочин, правоохоронні органи, транснаціональна кіберзлочинність.*

Summary. *The article deals with the issues of international cooperation in counteraction to transnational cybercrimes. The proposals on improvement of cooperation between domestic law enforcement agencies and foreign partners are formulated in order to increase the efficiency of the investigation of cybercrime.*

Keywords: *international cooperation, cybercrime, law enforcement agencies, transnational cybercrimes.*

Аннотация. *В статье исследуются вопросы международного сотрудничества в борьбе с транснациональной киберпреступностью. Сформулированы предложения по усовершенствованию сотрудничества отечественных правоохранительных органов с иностранными партнерами с целью повышения оперативности расследования соответствующих преступлений.*

Ключевые слова. *Международное сотрудничество, киберпреступление, правоохранительные органы, транснациональная киберпреступность.*

Постановка проблеми. Міжнародне право має численні джерела, які прямо або опосередковано регламентують співробітництво правоохоронних органів у боротьбі з транснаціональною кіберзлочинністю. Основним таким документом безумовно є Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. (далі – Конвенція), яка спрямована на підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов’язаних з комп’ютерними системами і даними, на надання можливості збирання електронних доказів тощо [1]. Зазначена Конвенція має не регіональний, а фактично міжнародний характер.

Конвенція про боротьбу із злочинами у сфері інформаційних технологій Ліги арабських держав від 21 грудня 2010 р. та Угода про співробітництво в сфері забезпечення міжнародної інформаційної безпеки Шанхайської організації співробітництва від 16 червня 2009 р. мають регіональний характер і також спрямовані на боротьбу з транснаціональною кіберзлочинністю.

Однак міжнародна спільнота намагається сформувати додаткові правові і організаційні передумови для підвищення ефективності протидії транснаціональній кіберзлочинності. Наприклад, у лютому 2016 року ЄС та НАТО підписали технічну угоду щодо посилення співпраці у сфері кібербезпеки, спрямованої на створення сприятливих умов задля оперативного обміну інформацією та досвідом між командами екстреного реагування НАТО “Computer Incident Response Capability” (NCIRC) та ЄС

“Computer Emergency Response Team of the European Union” (CERT-EU) у сфері протидії кібератакам, комплексного протистояння сучасним викликам у кіберпросторі.

Для України особливої актуальності набуває досвід міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю, насамперед приклади результативної взаємодії правоохоронних органів у цій сфері.

Результати аналізу наукових публікацій свідчать про те, що питання співробітництва іноземних держав та їх правоохоронних органів у боротьбі з транснаціональною кіберзлочинністю були предметом досліджень лише частково. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як О. Бойченко, В. Брижко, В. Бутузов, А. Войціховський, В. Марков, В. Пилипчук, К. Тітуніна, М. Швець, О. Юрченко та інші. Автор розпочав розгляд дотичних питань у контексті проблем розслідування кіберзлочинів в Україні [2].

Метою статті є розкриття досвіду міжнародного співробітництва у боротьбі з транснаціональною кіберзлочинністю задля визначення можливостей його використання в Україні.

Виклад основного матеріалу. На сучасному етапі правоохоронні органи іноземних держав взаємодіють у межах розслідування транснаціональних кіберзлочинів переважно на підставах, передбачених ст.ст. 24 – 35 Конвенції у таких напрямках як: екстрадиція; взаємна допомога (як з метою розслідування злочинів, пов’язаних з комп’ютерними системами та даними, так і з метою збирання доказів у електронній формі щодо кримінального правопорушення); добровільна допомога (правоохоронний орган у межах національного законодавства без попереднього запиту надсилає іноземному партнеру інформацію, отриману в ході його розслідування, якщо вважає, що розкриття такої інформації може допомогти партнеру у відкритті або проведенні розслідування кіберзлочинів); взаємна допомога щодо тимчасових заходів, яка включає термінове збереження комп’ютерних даних, які зберігаються; термінове розкриття збережених даних про рух інформації; взаємна допомога щодо доступу до комп’ютерних даних, які зберігаються; транскордонний доступ до комп’ютерних даних, які зберігаються, за згодою або у випадку, коли вони є публічно доступними; взаємна допомога у збиранні даних про рух інформації у реальному масштабі часу; взаємна допомога у перехопленні даних змісту інформації; цілодобова мережа для обміну інформацією [1].

Важливе значення для співробітництва між державами у сфері боротьби з транснаціональною кіберзлочинністю мають двосторонні та багатосторонні міжнародні договори про взаємну правову допомогу, взаємне визнання іноземних судових рішень, адже на їх основі також відбувається співпраця між правоохоронними органами різних країн.

На сьогодні існує потреба прийняття на рівні ООН універсального міжнародно-правового акту, наприклад, Конвенції протидії кіберзлочинності. Окремі організаційні передумови для цього є. Так, Глобальна програма з кіберзлочинності, відповідно до резолюції Генеральної Асамблеї 65/230 і Комісії з попередження злочинності та кримінального правосуддя резолюції 22/7 і 22/8, передбачає допомогу державам-членам у їх боротьбі з кіберзлочинами, пов’язану переважно з технічною допомогою, яка фінансується за рахунок підтримки урядів Австралії, Канади, Японії, Норвегії, Великобританії і США [3]. Корисними для вітчизняних правоохоронців є ресурси репозиторію ″Cybercrime″, створеного у 2015 році в межах Комісії з попередження злочинності і кримінального правосуддя, який містить бази даних законодавства,

прецедентного права (понад 180 країн) про кіберзлочинність та електронні докази, судову практику, а також записи успішних правоохоронних операцій щодо кіберзлочинів та збирання електронних доказів [4].

Найрезультативнішим є співробітництво правоохоронних органів різних країн у межах Інтерполу, оскільки ця організація має унікальний статус, який передбачає поглиблення боротьби з кіберзлочинністю у глобальному масштабі шляхом активного вивчення нових злочинів, новітніх методів навчання та розробки інноваційних інструментів поліцейської діяльності. Інтерпол через свої Національні центральні бюро в 190 країнах здійснює координаційні зусилля, в першу чергу через підтримку національної поліції, полегшення обміну інформацією та надання оновлень щодо розслідувань [5].

Показовою є операція з протидії кіберзлочинам під проводом Інтерполу у взаємодії з Асоціацією держав Південно-Східної Азії (АСЕАН), яка призвела до виявлення майже 9000 серверів команд і керування та сотень зловмисних веб-сайтів, включаючи державні портали. Операція об’єднала слідчих з Індонезії, Малайзії, М’янми, Філіппін, Сінгапуру, Таїланду, В’єтнаму та Китаю, а також експертів з компаній приватного сектору: Trend Micro, Cyber Defense Institute, Booz Allen Hamilton, British Telecom, Fortinet та Palo Alto Networks та інших. Було виявлено близько 270 сайтів, заражених шкідливим кодом, які використовували вразливість у застосуванні дизайну веб-сайту. Серед них було кілька державних веб-сайтів, які могли містити персональні дані громадян, виявлено декілька операторів фішингу, зловмисне програмне забезпечення, зокрема спрямоване на фінансові установи, на DDoS-атаки та розповсюдження спаму. Операція допомогла учасникам виявити та розслідувати різні види кіберзлочинів, які раніше не розслідувались у країнах-учасниках операції, сприяла навчанню обробки реальної кіберінформації, наданої приватними компаніями та Інтерполом [6].

Правозахисне агентство ЄС, Європол, а також його Об’єднана робоча група з боротьби з кіберзлочинністю, яка також включає в себе представників ФБР та спецслужб США, співпрацюють разом у розслідуванні кібератак [7]. Так, міжнародна операція, спрямована на шахраїв з авіаквитками, призвела до затримання 153 осіб, підозрюваних у використанні квитків, придбаних за краденими, підробленими кредитними картками. Операція відбувалася з 6 по 8 червня 2017 року за участі 64 країн, 84 авіакомпаній та 8 онлайнових туристичних агентств, які співпрацювали з працівниками правоохоронних органів для здійснення оперативних заходів у 230 аеропортах світу. Всього було повідомлено про 312 підозрілих операцій. Представники авіакомпаній, он-лайнові туристичні агентства, компанії з обслуговування платіжних карток, платформа для огляду міжнародної туристичної індустрії Perseuss та Міжнародна асоціація повітряного транспорту (IATA) надавали додаткову інформацію про підозрілі транзакції під час операції. Операція була скоординована з операційних центрів у Європі в Нідерландах, глобальному комплексі інновацій Інтерполу в Сінгапурі та Америполом в Боготі. Її також підтримали UNODC (AIRCOP для Африки), канадські та американські правоохоронні органи. Шахрайські онлайн-покупки авіаквитків призводять до збитків авіакомпанії до 1 млрд. дол. США на рік, є прибутковими для організованої транснаціональної злочинності і часто сприяють більш серйозній злочинній діяльності, включаючи нелегальну імміграцію, торгівлю людьми, контрабанду наркотиків та тероризм [8].

Поліція використовує за допомогою фахівців приватного сектору нові методики виявлення та припинення діяльності транснаціональної кіберзлочинності. Так, у межах операції Avalanche здійснювалось “просіювання” шкідливого Інтернет-трафіку. Коли,

наприклад, заражений комп’ютер намагається зв’язатися з його контролером, поліція за допомогою спеціальної технології фіксує це повідомлення та перешкоджає його зв’язку із фактичним центральним контролером. Таким чином, заражений комп’ютер не може передавати протиправні команди. Однак переривання технологічних систем недостатньо для того, щоб поліція зупинила злочинців. Починаючи з 2010 року тричі поліція намагалася зняти ботнет Kelihos. Операція Avalanche призвела до арешту п’яти осіб, які були керівниками організації. Їх усунення від злочинних дій, призвело до тимчасового “збою” в глобальному середовищі кіберзлочинності [9]. До речі, Департаментом кіберполіції Національної поліції України у межах спецоперації Avalanche здійснювались заходи щодо затримання на території України одного з основних фігурантів зазначеного провадження [10].

Активно використовуються іноземними державами технологічні рішення для боротьби з транснаціональною кіберзлочинністю. Так, Європол представив членам ЄС систему IOCTA (Internet Facilitated Organised Crime Tread Assessment), яка сприяє розкриттю кіберзлочинів. На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів [11].

Показовим є наступний приклад трансатлантичної співпраці. Так, два провідні он-лайн-анонімні ринки – Alpha Bay і Hansa Market – були заблоковані Федеральним бюро розслідувань (ФБР) та Голландським національним відділом злочинності високих технологій (NHTCU) під час операції “Байонет” [12]. ФБР вдалося порушити роботу AlphaBay – відомого даркнету, а NHTCU втрутився на даркнет-ринок Hansa протягом майже місяця як адміністратор, а потім закрив Hansa Market назавжди. Багато користувачів AlphaBay шукали притулок на ринку Hansa, на якому на той момент працювало NHTCU. Отже, поліцейські установи були в ідеальному становищі, щоб не тільки порушити екосистему, створюючи недовіру серед користувачів на цих анонімних ринках, а й збирати цінні дані на тисячі з них [13].

Набуває розвитку протиправна діяльність із використання криптовалют. Так, за статистикою кібервідділу Національного Агентства по боротьбі зі злочинністю Великої Британії (NCA) у 2013 році було зафіксовано вчинення кримінальних правопорушень із використанням криптовалюти на суму еквівалентну 3 млн. доларів США, у 2016 році – вже понад 100 млн. доларів США. Трендом у Британії стало використання злочинцями у протиправній діяльності сервісів з анонімізації криптовалютних транзакцій та повністю анонімних цифрових валют. Враховуючи те, що в Британії діє прецедентне право, фахівцям кібер-відділу NCA, розслідуючи злочин із використанням цифрової валюти, вдалось отримати позитивний судовий прецедент. Так, при розгляді справи в суді оперативниками було подано клопотання про вилучення і подальшу реалізацію біткоїнів, отриманих злочинним шляхом. У мотиваційній частині клопотання британськими спеціалістами було зазначено про те, що криптовалюта є різновидом майна, а отже до неї можливо застосувати загальне законодавство про збирання доказів та вилучення доходів, отриманих злочинним шляхом. У подальшому, тільки у 2017 році в Британії NCA було здійснено понад 10 успішних випадків вилучення криптовалюти у межах кримінальних проваджень [14].

Позитивним для України є той факт, що починаючи з 2019 року NCA нададуть доступ до спеціального програмного забезпечення, за допомогою якого можливо ефективно відслідковувати проведені криптовалютні транзакції у межах розслідування кримінальних злочинів, у повному обсязі підрозділам СБ України та Департаменту кіберполіції.

Заслуговують на увагу підходи іноземних держав щодо створення інституційних і технологічних передумов для протидії транснаціональній кіберзлочинності. Так, у Казахстані передбачено створення глобальної системи інформаційної безпеки “Кіберщит”, яка буде захищати від кібератак державні інформаційні ресурси.

У Китаї вступив в силу Закон про кібербезпеку КНР, прийнятий у жовтні 2016 року. У ньому передбачені загальні принципи і заходи мережевої безпеки, зокрема нагляд, заходи попередження і реагування у випадках кібератак. Крім того, стандартизація і державний контроль є основою безпеки Інтернету в Китаї, що дає правові можливості на законних підставах виявляти і документувати транснаціональні кіберзлочини.

Стратегія кібербезпеки Європейського Союзу [16] передбачає здійснення кіберзахисту за такими напрямами:

- виявлення і блокування кібератак, локалізації їх наслідків незалежно від походження стосовно об’єктів усіх форм власності;
- виявлення і розслідування кіберзлочинів.

Виявлення і блокування кібератак здійснює Європейська агенція мережевої та інформаційної безпеки (European Network and Information Security Agency, ENISA), кібератаки виявляє підрозділ CERT-EU за допомогою спеціалізованої технологічної системи датчиків, встановлених на абонентських лініях доступу до серверів ІТС з інформацією, яка захищається, та центру збору інформації про кібератаки. У разі здійснення кібератаки спрацьовує датчик, про що оперативно сповіщається центр.

Виявлені CERT-EU кібератаки з ознаками злочинних дій чи розвідувально-підривних акцій передаються до Європейського центру з розслідування кіберзлочинів (European Cybercrime Centre, EC3), який надалі може поінформувати про них Європейську агенцію оборони (European Defence Agency, EDA) для організації кібероперацій або Європейську службу зовнішніх справ (European External Action Service) для реагування дипломатичними каналами [16; 17].

ENISA, Європейське оборонне агентство (EDA), Європол та Група з реагування на комп’ютерні надзвичайні ситуації для установ, органів та установ ЄС (CERT-EU) 23 травня 2018 року підписали Меморандум про взаєморозуміння, яким встановили основи співпраці між їхніми організаціями. ENISA, EDA, EUROPOL та CERT-EU почали дискусії в 2016 році, що в підсумку призвело до підпису Меморандуму про взаєморозуміння [18]. Такий механізм співпраці може бути актуальним і для відповідних відомств в Україні.

У нашій державі передбачено (ст. 14 Закону України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 р.) можливість надання Україною іноземній державі інформації з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю на підставі запиту, додержуючись вимог законодавства України та її міжнародно-правових зобов’язань. Така інформація може бути надана без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору. Подібні норми мають передбачати у національних правових системах й інші держави задля ефективної боротьби з транснаціональною кіберзлочинністю.

Насамкінець відзначимо, що у різних державах створюються спеціалізовані підрозділи правоохоронних органів для розслідування кіберзлочинів, збирання та аналізу електронних доказів. Адже з огляду на те, що робота з комп’ютерним

обладнанням вимагає спеціальних знань, кіберзлочини мають розслідуватись виключно співробітниками тих підрозділів правоохоронних органів, які мають спеціальні навички для ведення відповідних проваджень та пройшли підготовку.

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін. Серед основних функцій цих підрозділів виділяють:

- моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;
- здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;
- розслідування кіберзлочинів, надання методичної та практичної допомоги іншим органам, зокрема правоохоронним у межах своєї компетенції;
- накопичення, узагальнення та аналіз інформації про кіберзлочинність;
- профілактика кіберзлочинів за допомогою громадськості та засобів масової інформації;
- навчання працівників поліції [15, с. 109].

Висновки.

Для покращення рівня співробітництва вітчизняних правоохоронних органів із зарубіжними партнерами доцільно створити в Україні єдиний технологічний центр обміну інформацією про кіберзагрози між правоохоронними органами України, ЄС та НАТО. Такий центр імовірно має бути створений на платформі співробітництва України з Інтерполом і Європолом, що сформована на базі Департаменту міжнародного поліцейського співробітництва Національної поліції України. Існує потреба провадження у вітчизняну практику взаємодії з правоохоронними органами іноземних держав типових формалізованих документів інформаційного обміну для негайної передачі державі-стороні, яка потерпіла від транснаціонального кіберзлочину, з використанням мережі національних контактних пунктів.

Ефективними з огляду на завдання боротьби з транснаціональною кіберзлочинністю є запровадження міждержавного обміну інформацією із закритих хакерських форумів, яку отримують в США, Нідерландах, Франції, Великобританії, Канаді, інших державах, а також використання ресурсів репозиторію “Cybercrime” щодо законодавства понад 180 країн про кіберзлочинність та електронні докази, судову практику, а також успішні правоохоронні операції.

Перспективами подальших наукових пошуків визначаємо питання співвідношення інституту персональних даних і таємниці слідства під час розслідування кіберзлочинів.

Використана література

1. Про кіберзлочинність : Конвенція Ради Європи від 21 листопада 2001 р. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575
2. Марущак А.І. Проблеми розслідування кіберзлочинів в Україні / Економіка. Фінанси. Право. – 2018. – № 1. – С. 23-27.
3. Global Programme on Cybercrime. URL: https://www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html
4. Cybercrime Repository. URL: https://www.unodc.org/unodc/en/cybercrime/cybercrime-repository.html

5. The changing nature of cybercrime. URL: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

6. Interpol-led cybercrime operation across ASEAN unites public and private sectors. URL: https://www.interpol.int/News-and-media/News/2017/N2017-051

7. Building stronger international legal framework for cybercrime. URL: https://www.chathamhouse.org/expert/comment/building-stronger-international-legal-framework-cyb ercrime

8. 153 detained for ticket fraud following worldwide law enforcement operation. URL: https://www.interpol.int/News-and-media/News/2017/N2017-078, 13 June 2017

9. Police around the world learn to fight global-scale cybercrime. URL: http://theconversation.com/police-around-the-world-learn-to-fight-global-scale-cybercrime-75804

10. Офіційні дані Департаменту кіберполіції НПУ.

11. Threat Assessment on Internet Facilitated Organised Crime (IOCTA). URL: https://www.europol.europa.eu/activities-services/main-reports/threat-assessment-internet-facilitated-organised-crime-iocta-2011

12. Massive blow to criminal Dark Web activities after globally coordinated operation. URL: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

13. Rolf van Wegberg and Thijmen Verburgh. 2018. Lost in the Dream? Measuring the effects of Operation Bayonet on vendors migrating to Dream Market. In Proceedings of Workshop on the Evolution of the Darknet (WEBSCI). ACM, New York, NY, USA, 5 pages. URL: https://doi.org

14. Офіційні дані СБ України.

15. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності // Право і безпека. – 2015. – № 2(57). – С. 107-113.

16. Cybersecurity Strategy of the European Union : An Open, Safe and Secure Cyberspace / European Comission. High representative of the European Union for foreign affairs and security policy. – Brussels, 7.2.2013. – Join (2013) 1 final.

17. An evaluation Framework for National Cyber Security Strategies / Веб-сайт “European Union Agency for Network and Information Security”. URL: http://www.enisa.europa.eu

18. Four EU cybersecurity organisations enhance cooperation. URL: https://www.europol.europa.eu/newsroom/news/four-eu-cybersecurity-organisations-enhance-cooperation

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

УДК 004.056:341.48

ГУЦАЛЮК М.В., *доктор філософії (Ph.D.) з юридичних наук, доцент, с.н.с.,*
провідний науковий співробітник Міжвідомчого центру з проблем боротьби з організованою злочинністю при РНБО України

ПРОТИДІЯ ВИКОРИСТАННЮ УЧАСНИКАМИ ЗЛОЧИННИХ УГРУПОВАНЬ МЕРЕЖІ “ДАРКНЕТ”

Анотація. *В статті досліджуються питання протидії кіберзлочинності, зокрема використання мережі “Даркнет”. Пропонуються напрями вдосконалення чинного законодавства.*

Ключові слова*: кіберзлочинність, “Даркнет”, міжнародне співробітництво.*

Summary. *The article deals with the issues of cyber crime, and using the Darknet in particular. The improvements of the legislation in this area are proposed.*

Keywords: *cyber crime, Darknet, international cooperation.*

Аннотация. *В статье исследуются вопросы противодействия киберпреступности, в частности использование сети “Даркнет”. Предлагаются направления совершенствования действующего законодательства в данной сфере.*

Ключевые слова: *киберпреступность, “Даркнет”, международное сотрудничество.*

Постановка проблеми. Поширення діяльності в Інтернеті найрізноманітніших верств населення по всьому світу та використання ними новітніх інформаційних технологій останнім часом відзначається значним зростанням кіберзлочинності.

Відповідно до звіту однієї з провідних компаній з інформаційної безпеки “Herjavec Group” активність кіберкриміналітету у найближчі десятиліття стане одним з найбільших викликів для людства. У 2021 році передбачається зростання щорічних збитків від кіберзлочинності в розмірі 6 трлн доларів США (порівняно з 3 трлн. у 2016 році). Це більше ніж прибуток від усієї глобальної незаконної торгівлі наркотиками [1].

Закон України “Про основні засади забезпечення кібербезпеки України” від 05 жовтня 2017 р. № 2163-VIII визначає кіберзлочинність як сукупність кіберзлочинів. У свою чергу кіберзлочин або комп’ютерний злочин визначено як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2].

До таких злочинів слід віднести правопорушення, передбачені розділом XVI КК України “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” (ст. 361-363). Також до даної категорії слід віднести і інші злочини, наприклад, передбачені ч. 3 ст. 190 (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки); ст. 200 (використання підроблених електронних засобів доступу до банківських рахунків); ч. 4 ст. 301 (збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки) КК України. На нашу думку, законодавець повинен надати чіткий перелік таких злочинів, що дасть можливість проведення якісного аналізу статистичних даних з метою вироблення стратегії і тактики протидії кіберзлочинності.

Інформаційні ресурси, як державні, так і приватного сектору, а також громадян, постійно піддаються різноманітним кіберзагрозам. Однією з найнебезпечніших кіберзагроз є кібератаки. В європейському законодавстві діє Директива щодо кібератак на інформаційні системи (Directive 2013/40/EU Of The European Parliament And Of The Council, of 12 August 2013) [3], у якій зазначається, що кібератаки на інформаційні системи, зокрема, пов’язані з організованою злочинністю, є зростаючою загрозою в Європейському Союзі та у всьому світі. Це, в свою чергу, призводить до зростання занепокоєння з приводу потенційних терористичних або політично мотивованих нападів на інформаційні системи, які є частиною критичної інфраструктури держав-членів Союзу.

Водночас організовані злочинні угруповання у своїй діяльності широко використовують мережу “Даркнет” (Darknet), веб-сайти якої не індексуються і на них не можливо потрапити через Google чи Yahoo. Ця частина Інтернету ніяк не врегульована законодавчо, діяльність у ній майже неможливо проконтролювати, а тому криміналітет на основі цієї мережі постійно створює і удосконалює протиправну діяльність.

Результати аналізу наукових публікацій. Дослідженням проблемних питань протидії кіберзлочинності займалися такі вітчизняні науковці, як Н.М. Ахтирська, П.Д. Біленчук., К.І. Бєляков, В.М. Бутузов, В.Д. Гавловський, М.А. Погорецький, В.Г. Хахановський, В.П. Шеломенцев, О.М. Юрченко та інші. Проте стрімкий розвиток інформаційних технологій та способів і методів протиправної діяльності у кіберпросторі спонукає для подальших досліджень.

Метою статті є визначення проблем протидії використання організованими угрупованнями мережі “Даркнет”, а також напрацювання відповідних пропозицій для ефективної протидії кіберзлочинності.

Виклад основного матеріалу. Міжнародна спільнота розпочала активну протидію кіберзлочинності, включаючи міжнародну, наприкінці минулого століття. Тоді в різних країнах були прийняті перші закони, в яких передбачена кримінальна відповідальність за відповідні правопорушення, створені спеціалізовані правоохоронні підрозділи. У 2001 році у Будапешті була прийнята Конвенція про кіберзлочинність [4], яка була ратифікована Верховною Радою України із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.05 р. Конвенцією визначено декілька груп правопорушень, які відносяться до кіберзлочинів. Це зокрема:

– правопорушення проти конфіденційності;

– правопорушення, пов’язані з комп’ютерами;

– правопорушення, пов’язані зі змістом;

– правопорушення, пов’язані з порушенням авторських та суміжних прав.

Крім прийняття відповідного законодавства в багатьох країнах створюються спеціалізовані правоохоронні органи. Крім цього виникла необхідність тісного міжнародного співробітництва у цій галузі – адже кіберзлочинність не має кордонів. Зокрема дані питання розглядалися на Першому міжнародному конгресі з кіберзлочинності E-Crime London 2002 [5].

Слід зазначити, що організованість хакерів постійно зростає. Так, за оцінками деяких дослідників, ще 7 років тому 80 % хакерів діяли самостійно, а вже сьогодні 80 % їх входять до складу злочинних угруповань, які мають переважно транснаціональний характер.

У своїй діяльності такі групи широко використовують криптографічні технології мережевої анонімності і онлайн-розрахунків, які дозволили злочинцям створити чорний ринок, де продають і купують наркотики, крадені і контрафактні товари, дитячу

порнографію, зброю тощо. Такий електронний ринок в Інтернеті має назву “Даркнет”. Сам термін з’явився ще до появи Інтернету і означав високу ступінь анонімності в комп’ютерній мережі, яка досягалася завдяки використанню нестандартних протоколів та портів. Також злочинцями широко використовується “Діпвеб” (Deep Web) – мережа сайтів, які не індексуються пошуковими системами.

У “Даркнеті” існує велика кількість хакерських спільнот, які спеціалізуються у своїй діяльності за конкретними напрямами, наприклад, неправомірний доступ до комп’ютерних систем, продаж шкідливого програмного забезпечення (далі – ШПЗ), організація кібератак, викрадення та продаж персональних даних тощо.

Водночас сьогодні активно формується ринок хакерських послуг, завдяки якому відбувається поєднання традиційної злочинності, включаючи організовані її форми, з кіберзлочинністю – адже немає потреби бути фахівцем в сфері інформаційних технологій – достатньо замовити відповідні послуги через Інтернет та розрахуватися за послуги криптовалютою. Даний кіберринок постійно зростає завдяки анонімності на основі спеціальних протоколів зв’язку, реалізованих в цьому інтерфейсі.

Найбільш популярними у “Даркнеті” є так звані “Служби злому”, у яких хакера можна найняти для проникнення до облікових записів Gmail або Facebook чи іншого виду кібершпигунства.

Згідно розслідування “Business Insider” [6], вартість проникнення в аккаунт Gmail коштує близько 90 доларів. Вартість злому Facebook-акаунта становить 350 доларів

Іншими поширеними товарами у Діпвеб є курси хакера, які продаються за 20 доларів. В них розповідається про пошук основних уразливостей сайтів, DDoS атаки або методи пошкодження веб-сайтів.

Популярними також є навчальні посібники, що надають інструкції для злочинців та хакерів, які хочуть отримати знання з кардингу, інформацію про запуск комплектів експлойтів, керівництво по організації спаму та фішингу тощо. Хакерські спільноти дуже активно займаються продажем викрадених кредитних карток, щоб охопити ширші аудиторії та надавати спеціалізовані послуги за більш високими цінами.

Зазначимо, що якщо наймаються професійні команди хакерів, то використовується зв’язок, який здійснюється через кілька спеціалізованих сервісів. Тому справжніх виконавців відслідкувати досить важко, і у багатьох випадках хакери можуть просто не виконувати свої завдання.

Методи розрахунків на чорному ринку постійно змінюються. Це пов’язано з тим, що крадіжка криптовалют стає досить поширеним явищем. Відповідно до дослідження аналітичної компанії “Autonomous Research” за минулі роки з моменту появи криптовалют хакери викрали понад 1,2 млрд. доларів в еквіваленті Bitcoin та Ethereum. Постійне зростання кібератак на криптовалюту відзначає і компанія “Bloomberg” [7].

В зв’язку з постійно зростаючим впливом кіберзлочинності на інформаційне суспільство Європейський центр боротьби зі злочинністю Європолу щорічно готує звіт “Оцінка загрози організованої злочинності в Інтернеті” – IOCTA. В звіті IOCTA – 2017 зокрема зазначається, що “Даркнет” ринки є ключовим міжгалузевим інструментом для інших сфер злочинності [8] . Надаючи доступ для платіжних даних для здійснення різноманітних видів шахрайства та підробних документів, торгівлі людьми тощо, цей тіньовий ринок сприяє незаконному обігу наркотиків, зброї та матеріалів сексуальної експлуатації дітей та іншій протиправній діяльності.

Аналітичні матеріали для IOCTA готуються на основі роботи експертів Європолу, правоохоронних органів, партнерів з приватного сектору та наукового середовища. На жаль, в Україні такі дослідження ще не проводилися, хоча актуальність цієї

проблеми вкрай висока, адже українські хакери постійно розшукуються правоохоронними органами різних країн по всьому світу, починаючи від міжнародного злочинного угруповання “CarderPlanet”, яка діяла на початку 2000-х рр. Затримані в різних країнах громадяни України через завдані іноземним компаніям мільйонні збитки отримують великі (30 – 40 років) терміни позбавлення волі.

Серед успішних заходів щодо протидії організованій кіберзлочинності слід зазначити наступні:

У грудні 2015 року німецькі поліцейські з Лейпцига конфіскували велику партію наркотиків, яку продавали через “Даркнет”, загальною вагою більше 210 кілограмів. Експерти оцінили поставку в 4,25 мільйони доларів США.

У жовтні 2016 року пройшла масштабна поліцейська операція під назвою “Гіперіон”. У ній приймали участь правоохоронці з США, Британії, ЄС, Канади, Австралії, Нової Зеландії. В результаті лише у Швеції було ідентифіковано і затримано 3000 покупців наркотиків, 6 продавців були заарештовані та отримали десятирічні терміни в’язниці.

У грудні 2016 року поліція Мальти заарештувала членів організації злочинного угрупування за продаж через Інтернет підроблених купюр Євро. Банкноти по 20, 50 і 100 Євро продавалися за 30 % від їх номінальної вартості, а оплату можна було здійснити в біткоїнах. Було конфісковано 160 000 Євро.

У березні 2017 року ірландським поліцейським вдалося виявити контрабандиста, який торгував зброєю через Інтернет по всьому світу. Продавця було затримано в результаті спільної операції ФБР та ірландської митниці.

Окремо слід відзначити масштабну операцію за участі правоохоронців 30 країн з ліквідації кібермережі “Avalanche” у 2016 році, яка проходила за підтримки Центру боротьби з кіберзлочинністю Європолу (EC3) та Об’єднаної групи боротьби з кіберзлочинністю (J-CAT), а також Євроюсту та Європейської банківської федерації (EBF). Одночасно в багатьох країнах було заарештовано 178 осіб – співучасників організованої злочинної групи, яку організував та очолював громадянин України [9].

В 2018 році в США арештовано трьох українських громадян – Федіра Хладира (33 роки), Дмитра Федорова (44 роки) та Андрія Копака (30 років). Їх підозрюють у зламі тисячі комп’ютерних систем і викраденні мільйонів номерів кредитних карт клієнтів. Після чого хакери продавали інформацію за викуп [10].

Правоохоронці, постійно підвищуючи рівень своєї майстерності, вишукують все нові методи протидії кіберзлочинності.

Наприклад, в Канаді правоохоронці використовують спеціалізовану пошукову систему, яка аналізує інформацію з “Даркнету”. Завдяки використанню цієї системи у серпні 2016 року відбулося затримання жінки, яка придбала через Інтернет смертельний радіоактивний елемент Полоній-210.

У березні 2017 року поліція Данії повідомила, що розробила власну аналітичну систему під назвою EC3, яка порівнює активність у “Даркнеті” з криптовалютною активністю користувача. Результатом використання такої системи став арешт 150 користувачів, які придбали заборонені товари.

Поліцейський департамент в американському місті Бостон розробляє програму, яка аналізує дані з “Даркнет” та соціальних мереж. Даний інструмент допоможе протидії тероризму, торгівлі людьми та захистить дітей від педофілів у мережі. Програмне забезпечення допоможе визначити геолокацію можливих правопорушень у реальному часі.

Крім того, правоохоронні органи для протидії кіберзлочинності, згідно огляду Дослідницького інституту “RAND Europe” [11], використовують наступні методи:

1. Традиційні методи розслідування.

Як тільки слідчі виявляють активність, пов’язану з наркотиками в реальному світі, вони аналізують відповідний кіберпростір. Спостереження дозволяють визначити ті точки, де зустрічаються реальний і віртуальний світ. Наприклад, арешт члена організації злочинного угрупування Ульбрихта в 2013 році відбувся, коли він скористався загальнодоступною мережею Wi-Fi, що співпало з появою адміністратора Silk Road у віртуальному просторі.

2. Отримання даних з відкритих веб-сайтів.

Торговці наркотиками використовують свої глибоко законспіровані сайти тільки як магазини, займаючись пошуком клієнтів у загальнодоступних мережах. Це робить дилерів протиправної продукції більш уразливими. Тому власники загальнодоступних сайтів повинні передавати у поліцію будь-яку інформацію щодо протиправної діяльності на їх ресурсах.

3. Перехоплення поштових відправлень.

Правоохоронні організації працюють із компаніями доставки та поштовими відділеннями, щоб досліджувати підозрілі пакети. Поліцейські можуть також взяти номер підозрілого відправлення, щоб стежити за одержувачем.

4. Великі дані і самонавчання машин.

Використовуючи великі обсяги даних, поліцейські визначають зв’язки, які неможливо встановити іншими способами. Вони враховують IP-адреси та розміщують онлайн-інформацію, роблячи висновки і поступово налаштовують до аналізу штучний інтелект.

5. Відстеження грошових потоків.

Хоча криптовалюта біткоїн має високу ступінь анонімності, слабким місцем її є купівля або продаж цифрової валюти. Поліція може вимагати дані від криптобіржі, хто і коли здійснив транзакції з криптовалютою. Правоохоронні органи також співпрацюють з цією метою з банками.

6. Робота під прикриттям.

Поліцейські агенти в різних країнах входять до довіри до адміністраторів заборонених сайтів, а також зображують продавців або роздрібних та оптових покупців.

7. Злом.

Модифіковане на замовлення поліцейських або ФБР програмне забезпечення широко використовується для визначення користувачів Deep Web. Наприклад, саме таким чином було розкрито великий нелегальний форум кіберзлочинців. Спеціалісти ФБР внесли в нього програму, яка пересилала IP-адреси користувачів до відповідного підрозділу служби.

В Україні після потужних кібератак, які були спрямовані на об’єкти критичної інфраструктури, було прийнято низку заходів щодо посилення кібербезпеки та протидії кіберзлочинності. Зокрема це прийняття Стратегії кібербезпеки України, створення Департаменту кіберполіції, посилення спроможності нових структур завдяки західним партнерам, навчання кіберполіцейських та слідчих виявленню та розслідуванню кіберзлочинів [12].

Проте, кількість кіберзлочинів продовжує щорічно зростати. Але найбільше занепокоєння викликають використання “Даркнету” для поширення наркотиків, у тому числі серед юнаків та дітей. І хоча точну кількість таких правопорушень через високий рівень латентності визначити складно, масштаби проблеми впажають суспільство [13].

Висновки.

Необхідно зазначити, що більш ефективній боротьбі з кіберзлочинністю в Україні, особливо з організованими її формами, сприяло би посилення кримінальної відповідальності за вчинення зазначених злочинів. Через те, що покарання передбачене нормами чинного Кримінального кодексу, значно м’якше ніж покарання за аналогічні злочини в різних країнах, що призводить до формування в Україні протиправних угруппувань.

Доцільним було б прийняття змін до Кримінального процесуального кодексу України щодо внесення поняття “електронні (цифрові) докази та особливості роботи з ними” до рекомендацій експертів ЄС. Відповідні напрацювання у цьому напрямку проведені у Міжвідомчому науково-дослідному центрі з проблем боротьби з організованою злочинністю [14].

Необхідною умовою протидії кіберзлочинності залишається співпраця з зарубіжними партнерами та активізація роботи з такими організаціями як Європол та Євроюст.

В зв’язку з необхідністю оперативного обміну комп’ютерними даними з відповідними правоохоронними структурами різних країн необхідно вдосконалити механізми співпраці з провайдерами та процедурами офіційної передачі таких даних.

Потрібно також постійно підвищувати професійну підготовку українських правоохоронців як завдяки зарубіжним партнерам, так і на основі розробки спеціалізованих курсів для вищих учбових закладів та курсів перепідготовки [15].

Отже, анонімною діяльність користувачів “Даркнет” залишається тільки до того часу, поки правоохоронні органи не починають вживати ефективні контрзаходи.

Використана література

1. Cybercrime Damages $6 Trillion By 2021. URL: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016 (дата звернення 07.09.2018).

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.17 р. № 2163-VIII. – (База даних “Законодавство України” / ВР України). – Режим доступу : http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення 07.09.2018).

3. Directive 2013/40/EU Of The European Parliament And Of The Council, of 12 August 2013. URL: https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32013L0040 (дата звернення 07.09.2018).

4. Конвенція про кіберзлочинність. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 07.09.2018).

5. Gutsalyuk M.V. Fighting Cybercrimes. URL: http://www.crime-research.org/library/Gutsaluk.html (дата звернення 07.09.2018).

6. Here’s how easy it is to buy anything – legal or illegal – on the ’dark web’. URL: https://www.businessinsider.com/find-anything-on-dark-web-tor-internet-2016-11 (дата звернення 07.09.2018).

Hacking communities in the Deep Web. URL: https://resources.infosecinstitute.com/hacking-communities-in-the-deep-web/#gref

7. Cryptocurrency Attacks Are Rising. URL: https://www.bloomberg.com/news/articles/2018-05-29/cryptocurrency-attacks-are-rising-as-rouge-miners-exploit-flaw (дата звернення 07.09.2018).

8. Internet Organised Crime Threat Assessment (IOCTA) 2017. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (дата звернення 07.09.2018).

9. В Україні затримали організатора хакерської мережі Avalanche. – Режим доступу : https://www.dw.com/uk/в-україні-затримали-організатора-хакерської-мережі-avalanche/a-42738720 (дата звернення 07.09.2018).

10. У США арештували українських хакерів. – Режим доступу : https://www.pravda.com.ua/news/2018/ 08/1/7188031 (дата звернення 07.09.2018).

11. The Hackers’ Bazaar : Markets for Cybercrime Tools and Stolen Data. URL: https://www.rand.org/events/2016/05/24.html (дата звернення 07.09.2018).

12. DR Mykhaylo Gutsalyuk. Ukraine’s Cybersecurity strategy and ways to implement it // European Cybersecurity journal. – Volume 2 (2016). – P. 65-69. – (The Kosciuszko Institute. Poland). URL: https://twitter.com/i/moments/781827366100140032 (дата звернення 07.09.2018).

13. Масштабы ужасают: в “Даркнете” работает крупная наркобиржа Украины. – Режим доступу : https://newsonline24.com.ua/masshtaby-uzhasayut-v-darknete-rabotaet-krupnaya-narkobirzha-ukrainy (дата звернення 07.09.2018).

14. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М.В. Гребенюк, В.Д. Гавловський, М.В. Гуцалюк, В.Г. Хахановський та ін.] ; за заг. ред. М.В. Гребенюка. – К. : МНДЦ при РНБО України, 2017. – 76 с.

15. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів : навч. посіб. / Н.М. Ахтирська . – К. : ВПЦ “Київський університет”, 2018. – 229 с.

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

Інформація в інших галузях права

УДК 336.711.65

ВИШНЕВСЬКИЙ Є.І., старший економіст, Національний банк України

РЕГУЛЮВАННЯ ТА НАГЛЯД В ФІНАНСОВІЙ СФЕРІ: МОДЕЛЬ “ТВІН ПІКС”

Анотація. *В статті досліджуються питання оптимальної моделі регулювання та нагляду в сфері фінансової діяльності. Систематизується та аналізується теорія та практика використання моделі “Твін пікс”.*

Ключові слова: *фінансове регулювання, глобальна фінансова криза, модель “Твін Пікс”.*

Summary. *The article explores the questions of an optimal model for regulation and supervision in a finance sphere. The theory and practice of the “Twin Peaks” model is systematized and analyzed..*

Keywords: *financial regulation, Global Financial Crisis, the “Twin Peaks” model.*

Аннотация. *В статье исследуется вопрос оптимальной модели регулирования и надзора в сфере финансовой деятельности. Систематизируется и анализируется теория и практика использования модели “Твин пикс”.*

Ключевые слова: *финансовое регулирование, глобальный финансовый кризис, модель “Твин Пикс”.*

Постановка проблеми. Глобальна фінансової криза 2007 – 2008 років не тільки показала певні слабкі сторони сучасної фінансової системи, а і звернула увагу на проблеми, які повинні бути вирішені у майбутньому.

На сьогодні різні експерти, залежно від їх спеціалізації, бачать ці проблеми по різному. Деякі з них фокусуються на переоцінці впливу фінансових посередників/ агентів на економіку [1]. На їх думку, уряди та центральні банки використовують макроекономічні моделі, що відомі як DSGE (Dynamic stochastic general equilibrium), які не включають ні банків, ні фінансових агентів. Вони фактично не включають фінансові системи як такі взагалі.

Нобелівський лауреат, економіст Пол Крагмен (Paul Krugman) визначив комплекс проблем, що виникли у зв’язку з фінансовою лібералізацією. Він визнав поразку економістів у прогнозуванні кризи у зв’язку з тим, що в їх економічних моделях *“вони були сліпими до обмежень людської раціональності, що часто призводять до бульбашок та колапсів на ринках; до проблем інститутів, що стали некерованими; до недосконалості ринків, особливо фінансових, що можуть спричинити несподіваний, непередбачуваний крах операційної системи економіки; і до небезпек, що виникають, коли регулятори не вірять у регулювання”* [2].

У звіті 2009 року “Фінансова реформа: база для фінансової стабільності” G-30 [3] (робоча група з Фінансової реформи Групи Тридцяти) визначила, що для досягнення надійності та стабільності фінансової системи необхідно сфокусуватись на способі організації її структури [4]. Хоча подекуди головні причини кризи ще не подолані, світові фінансові організації та місцеві регулятори серйозно поставились до цього питання і почали повномасштабні реформи фінансового сектору. На передньому плані таких змін постало питання стосовно інституцій, відповідальних за фінансове регулювання та

нагляд, частково через їхню неспроможність передбачити та подолати кризу і частково тому, що структурні моделі/архітектура таких органів не допомагали подолати кризу. Фактично це процес, що розпочався у світовому масштабі у 1995 у Великобританії. Він фокусується на пошуку найбільш підходящої моделі, що боротиметься з викликами фінансової системи і в той же час забезпечить шлях тривалого економічного зростання у майбутньому.

На додаток, G-30 визначила *“різноманітні підходи до регулювання та нагляду”*, які передбачали*“...поглянути на очевидні зміни на фінансових ринках і еволюцію структури нагляду локального рівня в часи, коли національні банки та наглядові агенції шукали шляхи покращення процесів нагляду у світлі розмивання кордонів між різними фінансовими сферами та бізнесом”* [5]. Відповідно до дослідження у 2008 році, модель регулювання та нагляду “Твін пікс”[1] була відзначена як “оптимальний інструмент забезпечення значної пріоритетності питань прозорості, ринкової цілісності і захисту споживачів” тобто, як одна з найбільш ефективних моделей управління ризиками фінансових ринків у світі. Таких підхід – *“...форма* (фінансового – *від авт.*) *регулювання за об’єктом, є такою, в якій існує розділення регулятивних функцій між двома регуляторами* (тобто агенціями – *від авт.*)*: однією, що виконують функцію нагляду за безпекою і надійністю, та іншою, що фокусується на регулюванні ведення бізнесу”* [5].

Проте на сьогодні ще продовжують мати місце багато питань щодо ефективності застосування моделі регулювання та нагляду “Твін пікс”.

Метою статті є узагальнення та дослідження теоретичних і практичних аспектів використання моделі “Твін пікс” для відповіді на питання, чи найкращим чином реагує ця система на сучасні виклики у фінансовій сфері.

Виклад основного матеріалу. Дебати стосовно фінансового регулювання в цілому і форм нагляду та їх жорсткості, зокрема, насправді ніколи не стихали. Після кожної кризи такі дискусії спалахували з новою силою. Одним з тих, хто задав тон сучасним розмовам про фінансове регулювання та нагляд, є доктор Чарльз Гудхарт (Charles Goodhart). Згідно з його працею “Яким чином ми повинні регулювати фінансовий сектор?”, фінансове регулювання завжди характеризувалось дуже практичною реакцією державних органів на термінові проблеми для уникнення їх повторення у майбутньому [6]. Фактично, структура/модель системи регулювання, що встановлює певні норми, принципи та вимоги, є дуже залежною від усвідомлення того, який нагляд повинен здійснюватися. Протягом довгого періоду часу вважалося, що індивідуальний ризик інститутів є потенційно найбільш небезпечним для стабільності фінансової системи. Відповідно, минула система була побудована з метою мінімізації такого роду ризику. Однак, як показала практика, фокусування нагляду на індивідуальному, а не на системному ризику інститутів, спричинило подальший крах системи. Гудхарт погоджується, що таким чином фінансовий нагляд у минулому був спроектований неякісно і показав свою нездатність гарантувати безпеку фінансової системи. Сучасний нагляд, на його думку, повинен в основному звертати увагу на системні зовнішні фактори та на захист споживача. Крім того, вважаю важливим те, що Гудхакрт поклав в основу доказів ідею “зміни парадигми”, тобто необхідності фундаментальних змін у розумінні державними органами мети фінансового нагляду. Таким чином, такий перегляд цілей фінансового нагляду призведе до змін в інструментах регулювання, тобто він змінить структуру/модель фінансового регулювання.

[1] “Твін пікс” (англ. – Twin Peaks – “дві вершини”) – визначається як “система подвійного регулятора/наглядовця ринків банківського, страхового та цінних паперів: один регулює практику ведення бізнесу/захист споживачів, інший відповідає за стабільність фінансової системи”.

Справедливим буде зазначити, що робота Гулхарта робить великий внесок у вивчення фінансового нагляду, хоча вона є частково теоретичною та вимагає певних емпіричних доказів.

Відповідно до Донато Мачіандаро (Donato Masciandaro) та Марка Куінтінса (Marc Quintynthe), зміни в структурі банківського регулювання траплялися часто як результат крахів на фінансових ринках або структурних змін на ринках. Вони аналізували емпіричним шляхом еволюцію регулятивних систем декількох країн протягом 1998 – 2008 років у своїй роботі “Після Великого вибуху і до наступного? реформування структури фінансового нагляду та роль центрального банку. Огляд світових тенденцій, причин та результатів (1998 – 2008)” [7]. Експерти дійшли висновку, що існувала тенденція структурних змін у банківському регулюванні та нагляді. Зокрема, це був початок переходу від моделі регулювання за секторами до уніфікованої (інтегрованої) моделі. Як результат такої хвилі реформ, виникла картина нагляду, що була диверсифікованою у такій мірі, як ніколи раніше. Хоча головний поштовх до масштабних реформ по всьому світу йшов з Великобританії, де у 1998 році було засновано Державний орган фінансових послуг, ця країна не була першою, хто впровадив цю модель. Скандинавські країни, Норвегія, Ісландія, Данія та Швеція здійснили зміну моделі банківського регулювання та нагляду в пізніх вісімдесятих – ранніх дев’яностих роках двадцятого століття. Мачіандаро та Куінтінс зазначали, що через нещодавню глобальну фінансову кризу реформи у структурі банківського регулювання та нагляду продовжуватимуться з переходом на моделі, що дадуть змогу регуляторам отримати доступ до вичерпної та актуальної ринкової інформації.

Висока важливість структури системи регулювання була прийнята до уваги світовою спільнотою. Експерти, міжнародні організації та високопосадовці цікавились роллю відповідної структури нагляду для забезпечення надійності фінансової системи. Серед інших видатних досліджень, велику роль у вивченні цього питання відіграють дослідження та конференції Світового банку. Базуючись на результатах конференції “Регулювання структур фінансового нагляду з урахуванням потреб країни”, що відбулася 4 – 5 грудня 2003 року та на якій було присутньо більш ніж 70 учасників з 52 країн, Джефрі Кармайкл (Jeffrey Carmichael), Александр Флемінг (Alexander Fleming) та Девід Т. Левеллін (David T. Llewellyn) видали однойменну книгу [8]. Автори, підсумовуючи інформацію, викладену на конференції, дійшли до висновку, що більшість країн розглядають структуру нагляду та регулювання як основний аспект результативності та ефективності. Іншим важливим нюансом, зазначеним у книзі, є той факт, що хоча не існує структурної моделі, яка б ідеально підходила кожній країні, було зазначено два протилежні підходи до побудови структури нагляду. З одного боку – традиційний нагляд за кожним сектором окремо, з іншого – підхід повної секторальної інтеграції. Розвинуті країни схилялися до того, щоб мати інтегрований нагляд. Тим часом, країни, що розвивалися, віддали перевагу секторальному регулюванню. Необхідно підкреслити, що структура регулювання та нагляду, як помітили автори, також дуже залежить від культурних та законодавчих традицій країни. Крім того, мають місце важко передбачувані фактори, які у результаті можуть мати певний вплив на модель регулювання та нагляду, як наголошують автори (наприклад, бажання влади мінімізувати витрати).

Один з рецензентів вищезазначеної книги Майкл Тейлор (Michael Taylor), дуже відомий експерт у сфері структури нагляду, був одним з перших, хто вивчав питання модернізації структури фінансового регулювання та нагляду. У 1995 році він написав звіт про модель регулювання “Твін пікс”, де підкреслив основні теоретичні аспекти моделі і запропонував, яким чином вона може бути використана на практиці у Великобританії та

передбачив майбутнє фінансового нагляду [9]. На додаток, Тейлор вказав на неефективність поєднання пруденційного регулювання та регулювання захисту споживача під одним дахом. У кінцевому рахунку цей звіт став книгою, обов’язковою для врахування у банківській справі, та популярним джерелом посилань.

Нещодавня глобальна фінансова криза разом з високою увагою на питання структури фінансового нагляду, змусили Тейлора приєднатися до дебатів про оптимальну структуру фінансового нагляду [10]. Головним спостереженням Тейлора, що стало важливим принципом, є те, що структура регулювання та нагляду повинна повністю відображати процеси, що відбуваються у фінансовому секторі. Він переконував, що традиційний секторальний нагляд більше не є ефективним для того, щоб регулювати фінансовий сектор через інтеграцію ринку цінних паперів, банківського ринку та ринку страхування. Тейлор пропонував регулювання за “об’єктами”. З цією метою, на його думку, найбільше усього підходила модель “Твін пікс”. Він розглядав два основні об’єкти моделі, незалежно від частини фінансової сфери. Перший повинен гарантувати надійність і стабільність усієї фінансової системи, другий – захищати споживача. Особливу увагу, відповідно до теорії Тейлора, необхідно звернути на системні фінансові інститути і на великі комплексні фінансові інститути. Він бачить шлях вирішення цього питання у накладанні спеціального податку на системний ризик на такі системні та великі комплексні фінансові інститути. В той же час, головні вимоги до капіталу для таких інститутів повинні бути вищими, ніж до інших. На додаток, він стверджує, що за великими комплексними фінансовими інститутами повинен бути нагляд шляхом трохи інших пруденційних норм, ніж для інших фірм. Хоча Тейлор зробив достатньо повний теоретичний аналіз моделі, він не використав жодного емпіричного (кількісного) доказу для того, щоб підтвердити свою точку зору. На нашу думку, фактично це робить його дослідження не досить повним. Подальші пошуки щодо ефективності моделі були здійснені, зокрема, в роботі Сон Вук (Sohn Wook) та Єгора Вишневського [11].

Серед всіх джерел слід відзначити звіт G-30 “Структура фінансового нагляду: підходи та виклики на світовій арені” [5]. Цей звіт присвячений вивченню певних національних підходів до нагляду та регулювання. Почавши огляд з липня 2007 року, G-30 хотіла побачити еволюційний процес структур національного регулювання. Група відзначила, що хоча системи нагляду в різних країнах мала справу зі схожими проблемами, їх підходи були різними. Це було викликано історичними, політичними, культурними, економічними і фінансовими розбіжностями кожної країни.

Робота виділяє чотири моделі фінансового регулювання у світі, а саме, інституційну, функціональну, інтегровану та “Твін пікс”.

Згідно зі звітом, інтерес до моделі “Твін пікс” швидко зростає. Фактично, такий вид регулювання включає багато переваг у порівнянні з іншими підходами. У звіті зазначається, що підхід “Твін пікс” може бути оптимальним засобом того, щоб питання прозорості, інтегрованості ринку та захисту споживача мали відповідний пріоритет”. Модель базується на принципах нагляду за об’єктом. Регулятивні та наглядові функції розділені між двома інститутами; один відповідальний за безпеку і надійність нагляду, а інший відповідальний за здійснення регулювання ведення бізнесу. На додаток, розділені роздрібна та оптова діяльність. Крім того, роздрібна діяльність регулюється наглядачем за веденням бізнесу.

Австралія була першою країною, що впровадила модель “Твін пікс”. З 1997 року країна розділила регулювання ведення бізнесу і пруденційного регулювання/нагляд. Таким чином, Австралійський орган пруденційного регулювання/нагляду (далі – АОПР)

регулює діяльність депозитних інститутів. Він фокусується на безпеці та надійності суб’єктів господарювання, що регулюються. Крім того, АОПР у своїй діяльності не залежить від центрального банку. Наглядачем за веденням бізнесу в Австралії є Австралійська комісія з питань цінних паперів та інвестицій (далі – АКЦПІ). Вона відповідальна за захист споживача та інтеграцію ринку у австралійській фінансовій системі. У цій системі нагляду, центральний банк Австралії, Австралійський резервний банк, відповідальний за фінансову стабільність, платіжні системи та процентні ставки. Фактично, австралійська модель фінансового регулювання відома як найбільш підходящий приклад практичного використання моделі “Твін пікс”.

Гострий інтерес до питання фінансового нагляду викликав ріст кількості якісних досліджень. Багато шкіл намагаються відповісти на питання “Яку модель обрати?” для отримання якісних результатів у регулюванні/нагляді. Першими, хто вивчав тему фінансового нагляду, а якщо бути більш точними, інтегрованого фінансового нагляду, були Мартін Чіхак (Martin Čihak) та Ричард Подп’єра (Richard Podpiera). Під час роботи у Міжнародному валютному фонді вони спромоглися разом зі Світовим банком створити систему унікальних даних про якість регулювання у світі. Згідно з дослідженням Чіхака та Подп’єра “Інтегрований фінансовий нагляд: яка модель?”, вплив моделі “Твін пікс” на якість нагляду сфери цінних паперів та інвестицій є досить схожим на вплив інших підходів до фінансового регулювання [12]. Тим часом, рівень наглядової якості в банківському секторі в середньому є вищим, коли модель використовується. Експерти дійшли висновку, що це спричинено кращою регулятивною практикою і більш високими стандартами пруденційного нагляду відповідно до принципів “Твін пікс”.

Слід відзначити, що Мартін Чіхак разом з Олександром Тіменом (Alexander Tieman) досліджували якість регулювання та нагляду фінансового сектору по всьому світу [13]. Аналогічно, як це було зроблено при написанні попередніх праць Чіхака, використовував унікальний пакет даних відповідності країн до міжнародних стандартів, що включав як теоретичну інформацію, так і детальну оцінку практичного впровадження загальноприйнятих міжнародних принципів та стандартів регулювання та нагляду фінансового сектору в кожній країні. Цікавим відкриттям є той факт, що у середньому регулятивні рамки країн відповідають міжнародним стандартам регулювання та нагляду фінансового сектору на рівні 75 відсотків. Також експерти виявили, що існує велика різниця у якості фінансового регулювання та нагляду в різних країнах. Це можна пояснити рівнем економічного розвитку. Фактично, якість систем фінансового нагляду економік з високим рівнем доходом вища, ніж у країнах з низьким або середнім рівнем доходу, хоча фінансові регулятори країн з високим рівнем доходу стикаються з більшими викликами, оскільки їх фінансові системи є більш комплексними.

Як показує огляд літератури, починаючи з часів, коли виникла проста фінансова система, питання того, яким чином здійснювати її нагляд і яким є найбільш ефективний шлях робити це, викликало значний інтерес. Суспільство одностайне у розумінні того, що немає ідеальної концепції/моделі регулювання та нагляду, однак, в той же час, різні країни різними шляхами приходять до достатньо схожих регулятивних моделей. Фінансова криза, що почалася у 2007 році, продемонструвала певні слабкі сторони структури/моделі фінансового регулювання. Таким чином, почався пошук нового шляху, більш підходящого для сучасних реалій. І сьогодні знаходження найбільш ефективної моделі регулювання та нагляду є важливою пріоритетною задачею не тільки для експертів та високопосадовців, але і для всього суспільства.

Як було вказано раніше, перший теоретичний огляд моделі “Твін пікс” було зроблено у 1995 році Майком Тейлором [9]. Даний підхід є реакцією на зміни на

фінансовому ринку, оскільки кордони між банківською діяльністю, страховим бізнесом та операціями з цінними паперами зникли, що зробило традиційну секторну модель регулювання та нагляду неефективною. Модель була спробою вирішити певні проблеми у фінансовій сфері, спричинені не тільки створенням великих фінансових холдингів, але і появою нових типів фінансових цінних паперів/інструментів та об’єднанням і роз’єднанням різноманітних видів послуг/продуктів, що раніше пропонувались інституційно іншими типами компаній [14].

Хоча деякі експерти класифікують модель як функціональний підхід до фінансового регулювання та нагляду (наприклад, Дік Шонмайкер (Dirk Schoenmaker) та Едді Вімерш (Eddy Wymeersch)) [15], більшість вважає, що “Твін пікс” є формою регулювання за об’єктом (тобто, в залежності від типу можливого збою ринкового механізму регулювання зобов’язане виправляти ситуацію). Головним питанням об’єктно-орієнтованого регулювання є зосередження на бажаному результаті або на об’єкті, використовуючи підходящу структуру регулювання (узагальнену модель нагляду за об’єктами див. на Рис. 1). Він дає певну гнучкість у досягненні цієї мети, певно, найкращим шляхом. Однак, такий підхід краще застосовувати як реакцію на зміни на ринку. Крім того, цей підхід може викликати ефект синергії у регулюванні та нагляді шляхом консолідування відповідальності у напрямах та може гарантувати вищій рівень дисципліни ринку.

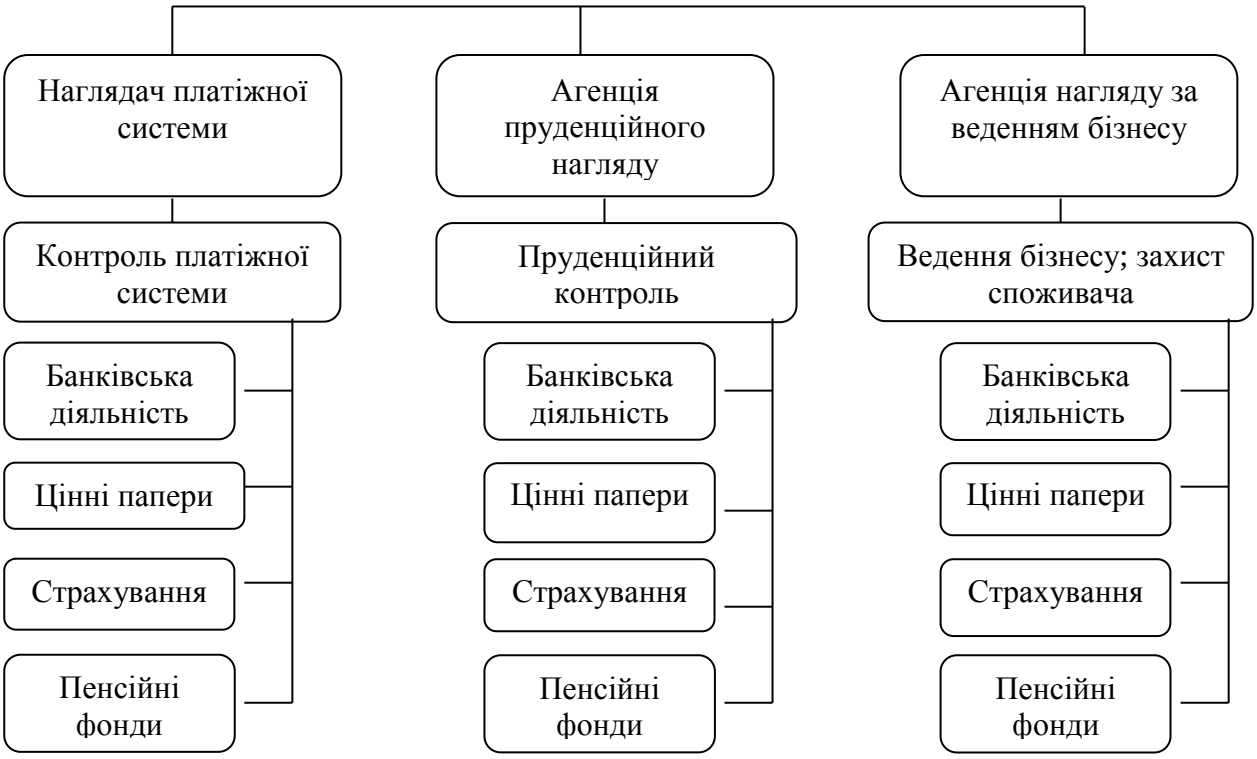


Рис. 1. Модель нагляду за фінансовими послугами за об’єктами (джерело: OECD – Organization for Economic Co-operation and Development [15])

Початково, підхід “Твін пікс” базується на розділення об’єктів регулювання та нагляду між безпекою і надійністю фінансової системи та порядком ведення бізнесу/ практикою (тобто захистом споживача). Насправді, справедливо буде сказати, що кількість об’єктів може бути більше ніж два. Деякі експерти виділяли чотири чи шість цілей регулювання та нагляду. Однак, з метою зменшення витрат на регулювання такі об’єкти були розділені на дві вищезазначені групи. Для того щоб досягти вищезазначених цілей,

Тейлор пропонував визначити дві агенції, незалежні від центрального банку. Закріплення різних об’єктів за окремими інституціями може мінімізувати конфлікт у суміжних сферах, тому що є вірогідність, що пруденційний мандат конфліктуватиме з питаннями ведення бізнесу, і регулятор може віддати пріоритет питанням безпеки та надійності, оскільки вони тісно пов’язані зі стабільністю фінансового сектору. Однак, навіть таке розділення не дає можливості уникнути напруження повною мірою, особливо коли пруденційні питання залишаються у пріоритеті до питань захисту споживачів.

Згідно з теорією Тейлора, навіть якщо така модель запущена у дію, роль центрального банку залишається життєво важливою, хоча його увага переключається з надійності окремих інститутів на підтримання стабільності функціонування секторів фінансового ринку та взаємозв’язків. Перш за все, центральний банк продовжує виконувати функцію органу, що проводить головну монетарну політику. В той же час, банк починає діяти як кризовий менеджер, якщо це потрібно. Його другим головним обов’язком є виконання макропруденційного регулювання та нагляду (тобто робота з системними ризиками, всеохоплюючою фінансовою структурою, процентною ставкою, платіжними системами тощо) та координація діяльності всіх регулюючих агенцій.

Відомо, що підхід “Твін пікс” є більш спеціалізованим ніж інші регулятивні моделі. Розділення регулятивних об’єктів на дві агенції надає їм можливість наймати спеціалістів відповідної компетенції для виконання їх спеціалізованих функцій [5]. Наприклад, пруденційний регулятор має можливість найняти персонал з конкретним діловим та фінансовим досвідом, коли регулятор ведення бізнесу фокусується на прийомі на роботу фахівців з відповідним досвідом. Це надає можливість вдосконалити загальну якість регулювання та нагляду.

Як це випливає з моделі, перша агенція має бути відповідальною за пруденційне, а якщо бути більш точними – мікропруденційне регулювання. Воно забезпечує тривалий фінансовий добробут фінансових компаній, що регулюються на індивідуальній основі. Зокрема, така агенція виконує дві основні функції. Перша – стимулювання безпеки та надійності страхових компаній, банків та інших фінансових інститутів шляхом забезпечення того, щоб спосіби, якими фінансові компанії здійснюють свою діяльність на ринку, не впливали або не загрожували стабільності всієї фінансової системи. Друга – мінімізація негативного впливу банкрутства компанії на таку стабільність, якщо таке трапляється.

Що стосується агенції, що відповідальна за питання ведення бізнесу, її головною метою є забезпечення захисту споживача на фінансовому ринку (тобто вирішення проблеми інформаційної асиметрії між споживачами фінансових послуг та фінансовими компаніями). На додаток така агенція повинна сприяти ефективній та чесній конкуренції та посилювати інтеграцію фінансової системи. Також агенція повинна сприяти зростанню впевненості у фінансовій системі у цілому (узагальнену модель класичного “Твін пікс” підходу надано на Рис. 2).

Фактично, ефективність моделі дуже залежить від підходящої управлінської структури, в якій повинні бути чітко встановлені всі функції, обов’язки, повноваження та зобов’язання всіх регулятивних агенцій. В той же час, для того щоб використовувати переваги моделі у повній мірі, комунікація та взаємодія між агенціями та центральним банком повинна бути постійною та взаємною.

Враховуючи вищенаведену інформацію про теоретичні засади моделі, стає можливим підсумувати переваги моделі.

По-перше, як зазначила G-30 у своєму звіті, модель “Твін пікс” може забезпечити швидкий та вільний потік інформації між відповідними агенціями та центральним банком, а також доступ широкої громадськості до інформації (тобто прозорість) [5].

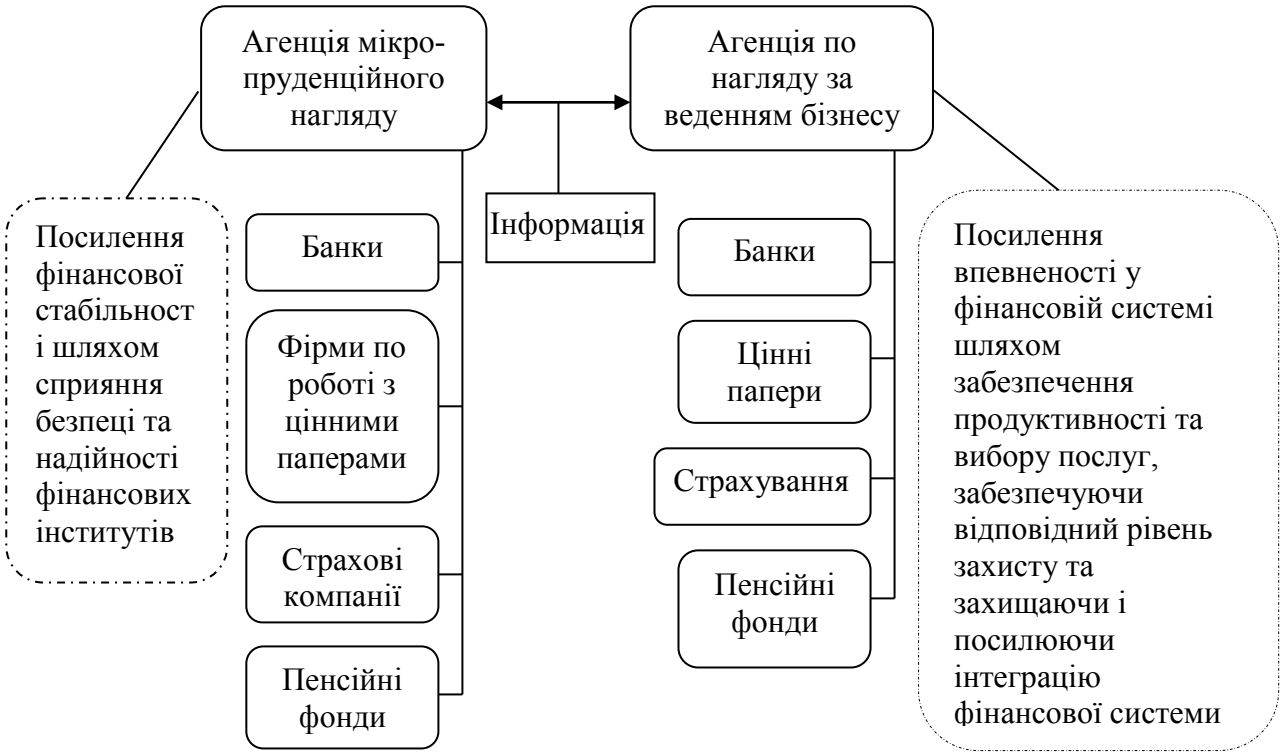


Рис. 2. Структура моделі класичної “Твін пікс” 1(джерело: KPMG [17])

По-друге, модель обмежує регуляторний арбітраж в рамках схожих фінансових послуг шляхом впровадження прямих та логічних норм та правил для аналогічних видів діяльності.

По-третє, завдяки моделі наглядовий орган може отримувати актуальну і вчасну інформацію про ризики стосовно регульованих компаній.

По-четверте, така регулятивна основа передбачає чіткі та зрозумілі об’єкти регулювання та нагляду (це означає, що наглядовий орган розуміє, хто є об’єктами нагляду та регулювання).

По-п’яте, “Твін пікс” надає можливість регуляторам якісніше визначати ризиковий напрям діяльності та застосовувати до такого напряму підходящі норми регулювання та нагляду, пропорційні до ризику.

По-шосте, підхід надає регуляторам можливість якнайшвидше виявляти потенційний ризик для споживачів та фінансової стабільності та усувати цей ризик. Та останнє, по-сьоме, підхід “Твін пікс” відповідає усім загальним міжнародним принципам фінансового регулювання та нагляду.

З часу її виникнення модель зазнала декількох змін та удосконалень. Наприклад, концепція розділення пруденційного нагляду на макро- та мікро- була інтегрована в модель після Азійської фінансової кризи 1997 – 1998 років, тому що до цього часу ідея макропруденційного нагляду ніяким чином не застосовувалась. Також після 2002 року, коли наглядові фінансові органи Нідерландів запровадили свою власну гібридну модифікацію моделі “Твін пікс”, стало зрозумілим, що модель являється достатньо гнучкою до будь-яких структурних змін та продовжує діяти ефективно. Головне удосконалення моделі було зроблено після глобальної фінансової кризи 2007 – 2009 років. Теоретичне та емпіричне переосмислення ролі у кризі фінансових холдингів, а саме системних та великих комплексних фінансових інститутів, змусило Тейлора вдосконалити модель. Окрім встановлення спеціального податку він запропонував запровадити

спеціальну комісію для регулювання бізнесу системних та великих комплексних фінансових інститутів. Ця комісія могла б бути дочірньою до центрального банку. При цьому, такі компанії стали б щонайменше потрійно регульовані. Крім того, Тейлор зазначав, що деякі фінансові компанії можуть бути вільними від пруденційного регулювання в залежності від розміру.

Сьогодні найбільш відомим та згадуваним прикладом впровадження моделі є австралійський досвід. Проте практичне застосування моделі “Твін пікс”, впровадженої у Нідерландах з 2002 року, показало певну ефективність. Фактично, нідерландська фінансова система є більш інтегрованою у глобальний фінансовий ринок ніж австралійська, що здійснює додатковий тиск на систему регулювання та нагляду. Крім того, в Нідерландах модель “Твін пікс” пройшла перевірку кризою.

До впровадження моделі у 2002 році нідерландська структура регулювання та нагляду була традиційною, на галузевій основі, з окремими органами нагляду за банківською діяльністю (центральний банк Нідерландів), страхуванням і пенсіями (Наглядач за страхуванням та пенсіями) та цінними паперами (Наглядач за цінними паперами, що був відповідальний за регулювання ведення бізнесу в рамках діяльності на ринку цінних паперів). З метою узгодження регулювання діяльності бізнесу та мікропруденційного регулювання між агенціями по нагляду на галузевій основі у 1999 році було засновано Раду фінансових наглядачів (свого роду міжсекторальний елемент). Завдяки послабленню кордонів між фінансовими компаніями, секторами фінансового ринку та фінансовими продуктами і послугами, спроможність такого підходу до регулювання зазнала невдачі. Три регулятори почати втрачати свою ефективність [15]. Під час цих процесів серед нідерландських політиків утворився консенсус стосовно необхідності фундаментальної реформи структури фінансового регулювання та нагляду. З того часу ключовим принципом фінансового регулювання та нагляду в Нідерландах є те, що розвиток фінансового ринку повинен бути відображений у максимальних змінах у структурі регулювання та нагляду.

Таким чином, була запроваджена реформа з фокусуванням на базі об’єктно-орієнтованого нагляду та регулювання фінансових агентів (її повне впровадження було закінчено у 2007 році). Спочатку голландські фінансові органи мали деякі переваги уніфікованого пруденційного нагляду. Це було спричинено змінами у структурі фінансового сектору Нідерландів. Слідом за світовими тенденціями великі фінансові холдинги вели свій бізнес у секторах фінансового ринку та пропонували комплексні фінансові сервіси та продукти, що були далеко за рамками традиційних кордонів таких секторів. У такому випадку, підпорядкування пруденційного регулювання та нагляду за банками, пенсійними фондами, страховими компаніями та компаніями по роботі з цінними паперами одному регулятивному інституту здавалося єдиним правильним вибором. На додаток, такий підхід також мінімізував регулятивний арбітраж. Таке бажання запровадити об’єктно-орієнтоване регулювання (з розподілом пруденційного регулювання та регулювання ведення бізнесу) привело нідерландські державні та фінансові органи до необхідності запровадження моделі “Твін пікс” [15]. При цьому, вони вирішили зосередити пруденційне регулювання та нагляд у центральному банку Нідерландів. Автори реформи очікувати досягти синергії, поєднуючи пруденційне регулювання та монетарну політику. Крім того, існує тісний взаємозв’язок між макроекономічною та фінансовою стабільністю. І як показала нещодавня фінансова криза, зосередження пруденційного контролю в центральному банку Нідерландів надає можливість мати картину системних питань в рамках усього фінансового ринку та швидко реагувати на кризу.

Вищезазначену логіку можна пояснити двома основними переконаннями державних та фінансових органів Нідерландів. По-перше, вони були переконані, що об’єкти пруденціного регулювання та регулювання ведення бізнесу цілковито відрізняються між собою, що вимагає дещо іншого комплексу навичок та іншої інституційної класифікації. По-друге, вони були впевнені, що стабільність фінансової системи повинна була бути тісно пов’язана з безпекою та надійністю індивідуальних фірм, а також з монетарною політикою (модель структури нідерландської системи регулювання та нагляду узагальнена на Рис. 3).

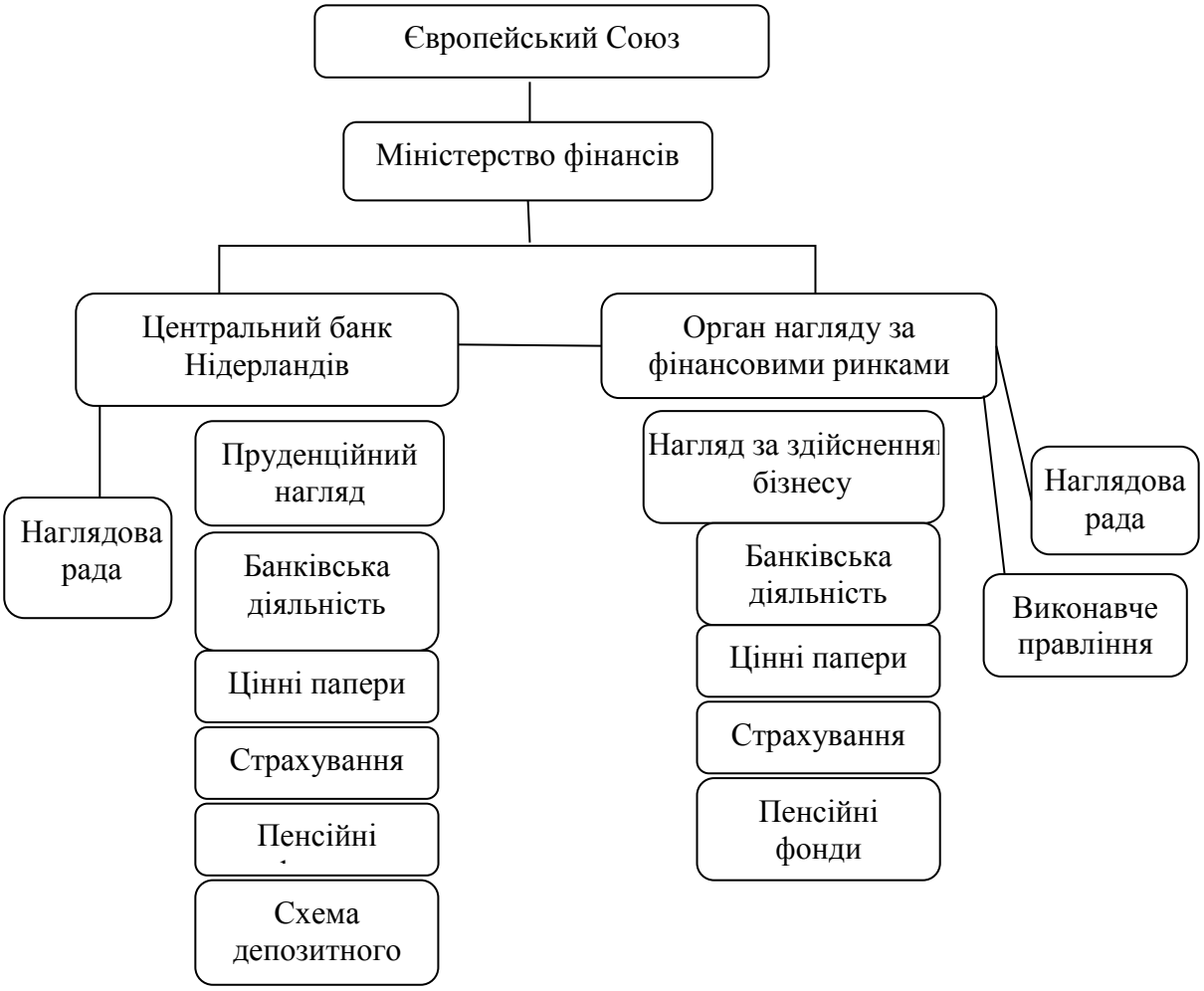


Рис. 3. Голландська модель фінансового регулювання та нагляду
(джерело: IMF – International Monetary Fund [18])

Головною відмінністю нідерландської моделі “Твін пікс” від класичної є те, що функції пруденційного (як макро-, так і мікро-) регулювання та нагляду виконуються центральним банком Нідерландів. І новозаснований наглядовий орган – Державна установа фінансових ринків, є відповідальною за нагляд за веденням бізнесу усіма фінансовими інституціями на ринку. Іншою специфічною характеристикою моделі є те, що центральний банк та Державна установа фінансових ринків мають достатньо обмежені права по нормотворчості, оскільки більшість норм та принципів були вже зазначені в Акті фінансового нагляду (2007 рік). У випадку, якщо з’являється необхідність внести якісь зміни у законодавчу базу, це може бути зроблено лише через указ Міністерства фінансів [15].

На практиці, інформаційний обмін та координація діяльності Центрального банку Нідерландів та Державної установи фінансових ринків регулюються “Зобов’язанням”, що забезпечує прозору базу для зобов’язань регуляторів, консультацій та взаємодії між ними. Також було встановлено роль Центрального банку як провідної агенції, відповідальної за повноцінне регулювання фінансових інститутів та Державної установи фінансових ринків як провідного регулятивного інституту для компаній по роботі з цінними паперами. На додаток, було погоджено, що провідний наглядач братиме до уваги позицію іншого наглядача (який теж має право вето).

Жерон Кремерс (Jeroen Kremers) та Дірк Шонмайкер (Dirk Schoenmaker), головні розробники структури фінансового регулювання та нагляду Нідерландів, як результат реформи підкреслювали два основні досягнення щодо якості регулювання та нагляду. По-перше, завдяки чіткому розділенню об’єктів нагляду між регуляторами, коли кожна інституція має свої власні чітко задекларовані об’єкти, всі сили цих регуляторів були витрачені більш ефективно та, відповідно, фокусувались тільки на полі їх відповідальності. По-друге, через покладення пруденційного регулювання на Центральний банк Нідерландів питання фінансової стабільності отримало більшу увагу регулятора. Також це дало центральному банку можливість бути більш ефективним при реалізації його монетарної політики, оскільки реакція ринку стала швидшою.

Стабільний розвиток моделі “Твін пікс” в Нідерландах довів свою спроможність при нещодавній кризі. Міжнародний валютний фонд у своєму звіті про нідерландську структуру фінансового регулювання та нагляду зазначив, що модель добре працювала протягом періоду глобального спаду світових фінансів [18]. Це було досягнуто завдяки прийняттю своєчасних рішень, а також частково завдяки можливості обміну інформації між агенціями. За правилами Міністерства фінансів, що координувало діяльність агенцій протягом кризи, група управління кризою встановила графік щоденних зустрічей. Вони включали представників з усіх агенцій фінансового регулювання. При цьому, завдяки прозорому розподілу сфер відповідальності агенцій, було досягнуто високого та ефективного рівня координації діяльності.

Тим не менш, криза показала декілька аспектів моделі, які повинні бути змінені для того, щоб використовувати переваги “Твін пікс” у повній мірі. Зокрема, могли проявитися деякі слабкі сторони моделі через те, що перехідний процес до моделі “Твін пікс” закінчився тільки у 2007 році (тобто було недостатньо часу для процесу вивчення моделі). По-перше, пруденційний регулятор сподівався використовувати метод “впливу шляхом переконання” протягом кризи, що був менш ефективним у порівнянні з примусовими заходами. По-друге, криза показала недоліки пруденційного регулювання системних та великих комплексних фінансових інституцій, таких як ING Group та Fortis. Кількість засобів для управління ними була обмеженою. І головна небезпека моделі була продемонстрована під час ситуації з ABN Amro у 2010 році. В той час в обох агенцій було запитано стосовно того чи голова банку, в минулому Міністр фінансів, Джерріт Залм (Gerrit Zalm) відповідав займаній посаді. Центральний Банк зробив висновок, що пан Залт відповідав займаній посаді, але Державна установа фінансових ринків мала протилежну думку. І проблема була в тому, що голландська модель “Твін пікс” не мала механізму для вирішення ситуації, коли обидва фінансові регулятори не можуть досягти згоди у деяких питаннях. Для вирішення того конкретного випадку Міністерство фінансів було змушене створити комісію. Тобто, голландські державні та фінансові органи влади визнали наявність проблеми і для її вирішення запровадили систему провідного наглядача в конкретних сферах. Однак, все ще залишається потреба у

згоді між регуляторами. На додаток, у звіті Голландського інституту вивчення державних витрат 2011 року зроблено висновок, що у сферах, де не чітко зрозуміло, який інститут має лідируючу позицію, існує ризик перетинання дій обох регуляторів. Також може статися, що якісь питання не будуть охвачені, оскільки обидва наглядача будуть вважати, що інший вирішує це питання.

На практиці, державні і фінансові органи Нідерландів наразі працюють над удосконаленням моделі фінансового регулювання та нагляду. Наприклад, Центральний банк вибрав проактивний та безумовний спосіб регулювання, шляхом створення управління правозастосовної політики в межах банку. Також макропруденційна лінія моделі була приведена у порядок шляхом створення управління макропруденційного нагляду в рамках департаменту фінансової стабільності центрального банку Нідерландів. В той же час ряд засобів макропруденційного регулювання було розширено. На додаток, розширення регулятивної бази усунуло різницю між регулювання банків та не-банків (тобто регулюванням тіньової банківської діяльності було приведено у порядок). Крім того, угода про “Зобов’язання” була удосконалена з метою скорочення можливості конфліктів між регуляторами та зміцнення взаємодії та обміну інформацією.

Висновки.

Підсумовуючи теоретичний та практичний огляд моделі регулювання відносин та нагляду в фінансовій сфері “Твін Пікс”, можна зробити декілька висновків.

По-перше, модель “Твін пікс” є ефективним інструментом управління поточними викликами фінансового ринку. Це було підтверджено її використанням, зокрема у Австралії та Нідерландах під час глобальної фінансової кризи. Голландський досвід показує, що розділення пруденційного регулювання/нагляду та регулювання ведення бізнесу має сенс та може добре працювати на практиці. Як вважаємо, комбінація мікро- та макропруденційного нагляду може покращити загальний рівень пруденційного нагляду. Також окремі агенції для пруденційного нагляду та регулювання ведення бізнесу можуть бути кращими в управління кризами.

Важливо те, що на практиці “Твін пікс” дозволяє уникнути ситуації коли одна агенція переважає над іншою. І останнє, криза показала на практиці сильні сторони моделі.

По-друге, модель є гнучкою та може адаптуватися до певних конкретних реалій або використовуватись частково.

По-третє, з’явившись у середині 90-х двадцятого століття, модель продовжує розвиватись та еволюціонувати для того, щоб відповідати сучасним вимогам фінансового регулювання та нагляду.

Дискусії щодо моделі регулювання “Твін пікс” продовжуються з 1995 року. З того часу модель була впроваджена у декількох країнах і результати її застосування тільки підтвердили її високу ефективність. Деякі країни, впевнені у працездатності моделі, вирішили застосувати її у своєму регулюванні фінансової системи.

Слід відмітити, що на сьогодні модель “Твін пікс” відома як найбільш ефективний шлях управління фінансовою системою, тільки подальший глибокий емпіричний аналіз використання моделі може надати відповідь на питання, чи найкращим чином реагує ця система на сучасні виклики фінансової системи.

Перспективи подальших наукових пошуків. На сьогодні модель “Твін пікс” відома як найбільш ефективний шлях регулювання та нагляду за фінансовою системою. Проте, тільки подальший глибокий емпіричний аналіз використання моделі може надати відповідь на питання, чи найкращим чином реагує ця система на сучасні виклики в фінансовій системі.

Використана література

1. New model army / The Economist, January 19, 2013. URL: http://www.economist.com/news/finance-and-economics/21569752-efforts-are-under-way-improve-macroeconomic-models-new-odel-army

2. Paul Kraugman. How Did Economists Get It So Wrong? / The New York Times, September, 2009. URL: http://www.nytimes.com/2009/09/06/magazine/06Economic-t.html?pagewanted=all&_r=0

3. The Group of Thirty is a private, nonprofit, international body composed of very senior representatives of the private and public sectors and academia. URL: http://www.group30.org – (офіційний веб-сайт G-30).

4. Working Group on Financial Supervision of Group of Thirty. Financial reform: a framework of financial stability, 2009. URL: http://group30.org/images/uploads/publications/G30_Financial ReformFrameworkFinStability.pdf

5. Working Group on Financial Reformof Group of Thirty. The Structure of Financial Supervision: Approaches and Challenges in a Global Marketplace, 2008. URL: http://www.group 30.org/images/PDF/The%20Structure%20of%20Financial%20Supervision.pdf

6. Turner, Adair et al. The Future of Finance: The LSE Report. – London : School of Economics and Political Science, 2010.

7. Masciandaro, Donato and Marc Quintyn. After the Big Bang and Before the Next One? Reforming the Financial Supervision Architecture and the Role of the Central Bank. A Review of Worldwide Trends, Causes and Effects (1998-2008). “Paolo Baffi” Centre Research Paper, Series No. 2009-37, January, 2009. URL: http://ssrn.com/abstract=1336390

8. Carmichael, Jeffrey, Alexander Fleming and David T. Llewellyn. Aligning financial supervisory structures with country needs. – Washington, D.C. : World Bank Institute, 2004.

9. Taylor, Michael. Twin Peaks: A Regulatory Structure for the New Century. – London : Centre for the Study of Financial Innovation, 1995.

10. Taylor, Michael. Twin Peaks Revisited: A Second Chance for Regulatory Reform. – London : Centre for the Study of Financial Innovation, September 2009.

11. Wook Sohn & Iegor Vyshnevskyi (2017). The Twin Peaks model of post-crisis banking supervision. Applied Economics Letters, 24:8, 571-574, DOI: 10.1080/13504851.2016.1213354. URL: https://www.tandfonline.com/doi/abs/10.1080/13504851.2016.1213354

12. Čihák, Martin, and Richard Podpiera. Integrated Financial Supervision: Which Model? / The North American Journal of Economics and Finance. Vol.19, no. 2 (2008): 135-152.

13. Čihák, Martin, and Alexander Tieman.Quality of Financial Sector Regulation and Supervision around the World / The IMF working paper, WP/08/190, August, 2008.

14. Schooner, Heidi M. and Michael Taylor. Regulation of global banking, principles and policies. – Burlington, MA : Academic Press, 2010.

15. Kremers, Jeroen and Dirk Schoenmaker. Twin Peaks: Experiences in the Netherlands. LSE financial markets group. November, 2010. URL: http://www.lse.ac.uk/fmg/workingPapers/ special Papers/PDF/SP196.pdf

16. Organization for Economic Co-operation and Development. The Financial Crisis, reform and exit strategies.2009. URL: http://www.oecd-ilibrary.org

17. KPMG. Twin Peaks regulation: key changes and challenges. November, 2012. URL: https://www.yumpu.com/en/document/view/10639076/twin-peaks-regulation-key-changes-and-better-regulation 18. International Monetary Fund. Kingdom of the Netherlands-Netherlands: Publication of Financial Sector Assessment Program Documentation–Technical Note on Financial Sector Supervision: The Twin Peaks Model. Country Report No. 11/208. – Washington, July 2011.

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

УДК 347.962

РОМАНІВ Х.Б., *кандидат юридичних наук,* доцент кафедри цивільно-правових дисциплін Львівського державного університету внутрішніх справ

ЗАБЕЗПЕЧЕННЯ ПРАВА НА СПРАВЕДЛИВИЙ СУД: МІЖНАРОДНЕ ЗАКРІПЛЕННЯ ТА ВІТЧИЗНЯНІ ЗДОБУТКИ

Анотація. *У статті досліджується поняття “права на справедливий суд”, розглядається зміст цього права в об’єктивному та суб’єктивному розумінні, визначаються структурні елементи цього права. Аналізується практика Європейського Суду з прав людини щодо розкриття змісту права на справедливий суд та її застосування вітчизняними судами. Робиться висновок щодо реалізації Закону України “Про забезпечення права на справедливий суд” та перспектив його подальшого впровадження.*

Ключові слова: *право на справедливий суд, рішення Європейського Суду з прав людини, імплементація, впровадження.*

Summary. *The article dwells upon the notion of “right to a fair trial”, the value of this right is considered in objective and subjective understanding, the structural elements of this right are determined. It analyses the practice of European court of human rights with regard to interpretation of right to a fair trial and its administration by national courts . The conclusion is drawn about the implementation of Law of Ukraine “On provision of right to a fair trial” and prospects of its further adoption.*

Keywords: *the right to a fair trial, the decision of the European Court of Human Rights, implementation.*

Аннотация. *В статье исследуется понятие “права на справедливый суд”, рассматривается содержание этого права в объективном и субъективном смысле, определяются структурные элементы этого права. Анализируется практика Европейского Суда по правам человека по раскрытию содержания права на справедливый суд и ее применения отечественными судами. Делается вывод о реализации Закона Украины “Об обеспечении права на справедливый суд” и перспективы для его дальнейшего применения.*

Ключевые слова: *право на справедливый суд, решения Европейского Суда по правам человека, имплементация, внедрение.*

Постановка проблеми. У контексті європейської інтеграції правовий статус суду та його місце у національній правовій системі було втілено шляхом прийняття Закону України “Про забезпечення права на справедливий суд” [1], який передбачає внесення змін до ряду законодавчих актів процесуального характеру. Прийняття цього закону стало точкою відліку впровадження принципу права на справедливий суд серед принципів здійснення судочинства.

Актуальність дослідження права на справедливий суд, його структурних елементів, практики Європейського Суду з прав людини щодо розкриття змісту права на справедливий суд є безсумнівною, адже ефективне впровадження цього права не може обмежитися лише прийняттям однойменного закону. Разом з тим, низка елементів забезпечення цього права, які були передбачені законом, не є впровадженими у здійснення судочинства.

Результати аналізу наукових публікацій. Окресленою проблематикою займалася низка науковців, серед яких: С. Афанасьєв, А. Бучик, Н. Грень, М. Ентін, Р. Куйбіда,

Т. Руда, М. Савчин, О. Ткачук тощо. Однак залишається малодослідженим аналіз практики Європейського Суду з прав людини щодо змісту права на справедливий суд.

Метою статті є з’ясування правової природи права на справедливий суд, витоків його формування та нормативного закріплення, передумов і особливостей його ефективності здійснення на базі аналізу практики Європейського Суду з прав людини.

Виклад основного матеріалу. Складність визначення поняття права на справедливий суд безпосередньо пов’язана із подвійною природою даного феномену. О. Ткачук визначає два напрямки, в яких дане право може знайти подальший розвиток: по-перше, як суб’єктивне право в контексті концепції прав людини, а по-друге, як система мінімальних вимог, дотримання яких має забезпечити держава під час звернення особи до суду, тобто як позитивне зобов’язання держави у сфері відправлення правосуддя в цивільних справах [2, с. 190]. Про неоднозначність визначення даного поняття свідчить і позиція Н. Греня, який стверджує, що “право на справедливий суд має комплексну структуру, складається з багатьох елементів і ототожнення цього права виключно з справедливою процедурою є не цілком вірним” [3, с. 248].

Підтримуючи позицію зазначених науковців, вважаю, що дане поняття слід розглядати у суб’єктивному та об’єктивному розумінні:

1) як особисте немайнове право, що забезпечує і можливість звернення до суду за захистом порушених, невизнаних, оспорюваних прав, і безпосередньо сам захист такого права незалежним та безстороннім судом;

2) як об’єктивно виражену систему гарантій, що забезпечують реалізацію такого суб’єктивного права особи.

Комплексний характер права на справедливий суд визначається насамперед із нормативного закріплення даного поняття у низці міжнародно-правових актів.

Так, у статті 10 Загальної декларації прав людини проголошується право кожної людини на те, щоб її справу було розглянуто прилюдно та з дотриманням усіх вимог справедливості незалежним і безстороннім судом [4]; стаття 14 Міжнародного пакту про громадянські і політичні права визначає право на справедливий і публічний розгляд справи компетентним, незалежним і безстороннім судом, створеним на підставі закону [5]. У статті 6 Конвенції про захист прав людини і основоположних свобод проголошується право на справедливий і публічний розгляд справи впродовж розумного строку незалежним та безстороннім судом, встановленим законом [6].

Комітет із прав людини та Європейський суд з прав людини (далі – ЄСПЛ) дотримуються різних позицій з приводу надання державам можливостей самостійно визначати зміст норм щодо справедливого судового розгляду в межах положень Міжнародного пакту про громадянські і політичні права та Конвенції про захист прав людини і основоположних свобод у внутрішньому законодавстві. Зокрема, на відміну від лояльних у визначенні даних питань рішень ЄСПЛ, які будуть проаналізовані далі, Комітет із прав людини дотримується безальтернативного підходу. У зауваженнях загального порядку № 32 про права на справедливий судовий розгляд зазначено, що у статті 14 містяться гарантії, яких держави-учасниці зобов’язані дотримуватись незалежно від їх юридичних традицій і національного права. Хоча вони повинні повідомляти, яким чином ці гарантії інтерпретуються в їх відповідних правових системах, Комітет зазначає, що основний зміст встановлюваних Пактом гарантій не може визначатись лише з огляду на положення національного права [7].

Будучи нормативно невизначеним та змістовно неоднорідним поняттям, питання про суть даного права та його структурні елементи викликає у науці безліч дискусій.

М. Ентін виділяє чотири структурні елементи права на справедливий суд: органічні, інституційні, процесуальні та спеціальні. До органічних при цьому відносить ті, що забезпечують ефективну реалізацію зазначеного права; інституційними є критерії відповідності визначеним стандартам судової системи держави загалом та кожного конкретного судового органу зокрема ; процесуальні – забезпечують реальну участь особи або її представника в розгляді справи, змагальність процесу, рівність сторін та розумні строки судового розгляду; спеціальні – це додаткові гарантії, визначені в пунктах 2 і 3 Конвенції та стосуються додержання універсальних вимог справедливого розгляду справи з урахуванням особливостей кримінального процесу [8, с. 87]. С. Афанасьєв дотримується аналогічної точки зору та розкриває зміст органічних елементів через механізми, які забезпечують ефективний доступ до правосуддя по цивільних та кримінальних справах і в однаковою мірою по виконанню рішень, а спеціальні елементи з його точки зору являють собою додаткові гарантії здійснення правосуддя з урахуванням особливостей кримінальної процесуальної діяльності. Вони необхідні для захисту прав суб’єктів, які підозрюються чи обвинувачуються у здійсненні кримінально караного злочину і до цивільного судочинства не відносяться [9, с. 23].

По-іншому структуру даного права визначає А. Бучик, яка виділяє в контексті даного права: право на доступ до суду, принцип рівності можливостей, незалежний та неупереджений суд, розумні строки розгляду, публічність розгляду справи, презумпція невинуватості, процедурні гарантії учасників правовідносин [10, с. 3-4].

Виходячи з конструкції ч.1 ст. 6 Конвенції, можна зробити висновок, що у ній закріплено такі елементи права на судовий захист:

1) право на розгляд справи;

2) справедливість судового розгляду;

3) публічність розгляду справи;

4) розумний строк розгляду справи;

5) незалежність та безсторонність суду, встановленого законом.

Беручи за основу критерій часової межі здійснення одного з вищенаведених процесуальних прав, вважаю, що такі можна поділити:

- ті, що пов’язані з можливістю звернення до суду;

- ті, що реалізуються в ході судового засідання.

До першої групи належить право на розгляд справи або право на доступ до правосуддя, що є визначальним та основоположним у судовому процесі. Зокрема, у справі *“Голдер проти Великої Британії”* Суд зазначив, що *“*конструкція права на справедливий суд була би безглуздою та неефективною, якби вона не захищала право на те, що справа взагалі буде розглядатися*”* [11]. Варто зазначити, що вітчизняні суди у своїй практиці при мотивуванні судових рішень посилаються на цю справу [12; 13]. Загалом, єдиний державний реєстр судових рішень налічує 126 кінцевих процесуальних документи у формі рішення чи постанови у цивільних та господарських справах.

У справі *“Салонтаджі-Дробняк проти Сербії”* (пункт 132) Суд зазначив, на “право на суд”, в якому право на доступ до суду є одним з його аспектів, може посилатися кожен, хто небезпідставно вважає, що втручання у реалізацію його або її прав цивільного характеру є неправомірним (рішення від 13 жовтня 2009 року) [14].

До другої групи належать усі інші процесуальні права, серед яких право на справедливий судовий розгляд, публічність розгляду справи та проголошення рішення; розумний строк розгляду справи; розгляд справи належним складом суду; незалежність і безсторонність суду тощо.

Однак, це лише приблизний перелік гарантій, які змістовно включають у себе право на справедливий суд. Кожна з держав-членів як суб’єкт імплементації міжнародно-правових актів, вправі на власний розсуд визначати зміст того чи іншого права. Зокрема, у справі *“Delcourt v. Belgium”* Суд зазначив, що “у демократичному суспільстві у світлі розуміння Конвенції, право на справедливий суд посідає настільки значне місце, що обмежувальне тлумачення статті 6 не відповідало б меті та призначенню цього положення” [15].

Таким чином, з огляду на універсальний характер, право на справедливий суд повинно слугувати дієвим засобом захисту інших прав особи. Фактично забезпечення даного права є основою організаційної діяльності суду та процедури вирішення ним юридично значущих справ. Основоположна роль і визначальне місце права на справедливий суд у контексті захисту прав людини вимагають належної імплементації цього інституту у національне законодавство та ефективного контролю за його здійсненням.

Протягом тривалого періоду розвитку вітчизняного законодавства право на справедливий суд взагалі не було закріплено у ньому.

Конституція України у статті 129 прямо не визначила принцип справедливості серед основних засад судочинства. Проте, окремі його складові передбачені у розділах І Загальні засади і ІІ Права, свободи та обов’язки людини і громадянина. Зокрема, у ст.55 Конституції України [16], як і у ст. 7 Закону України “Про судоустрій і статус суддів” [17], гарантовано право на судовий захист.

У Цивільному процесуальному кодексі України з моменту його прийняття завданням цивільного судочинства було визначено справедливий, неупереджений і своєчасний розгляд та вирішення цивільних справ із метою захисту порушених, невизнаних або оспорюваних прав, свобод чи інтересів фізичних осіб, прав та інтересів юридичних осіб, інтересів держави [18].

Новий етап у гарантуванні права на справедливий суд розпочався з прийняттям 12.05.15 р. однойменного Закону України “Про забезпечення права на справедливий суд” [1]. Можна сказати, що у цьому Законі відбулося безпосереднє закріплення “права на справедливий суд” як такого, хоч й в дещо обмеженому, порівнюючи з Конвенцією ЄСПЛ, вигляді.

Серед нововведень Закону слід виокремити наступні:

- запровадження конкурсного порядку добору на всі суддівські посади, зокрема й у суди вищого рівня;

- підвищено відкритість діяльності суддів, адже кожен отримав можливість здійснювати відеозапис судового засідання без спеціального дозволу суду, а усі без винятку судові рішення мають оприлюднюватися в єдиному державному реєстрі;

- посилено змагальність дисциплінарної процедури і запроваджено, замість двох, шість дисциплінарних стягнень: попередження, догана, сувора догана, тимчасове відсторонення від здійснення правосуддя (від місяця і до півроку), переведення судді до суду нижчого рівня та розгляд питання щодо звільнення судді з посади з підстав порушення присяги;

- забезпечено пряме оскарження рішень вищих судів до Верховного Суду.

Відповідно до висновків втілення конкретних рекомендацій Ради Європи у систему національного законодавства, Закон України “Про забезпечення права на справедливий суд” повністю врахував 27 рекомендацій у судовій сфері, ще 21 рекомендацію було враховано частково. Однак ключові рекомендації щодо обмеження політичного впливу Президента та Парламенту на судову систему, на жаль, було проігноровано [20].

Варто відзначити, що з моменту прийняття Закону України “Про забезпечення права на справедливий суд”, який повинен був стати точкою відліку реформування судової влади, минуло більше трьох років, а, отже, варто підводити певні підсумки. З реально закріплених у ньому елементів права на справедливий суд реально діючими є зміни до процесуальних кодексів, адже порядок проведення відеозапису судового засідання у всіх без винятку судах України змінився. Також можна вважати реалізованою норму закону про обрання суддів на адміністративні посади зборами суддів, а не їх призначення в адміністративному порядку. Протягом останнього року внаслідок формування на конкурсній основі складу Верховного Суду України було забезпечено пряме оскарження рішень вищих судів. Переатестація суддів всіх рівнів судової системи проходить завершальний етап.

Висновки.

Аналіз міжнародно-правового закріплення права на справедливий суд, розкриття змісту цього права Європейським судом з прав людини та його імплементації у національне законодавство дозволяють зробити наступні висновки. Попри недоліки, пов’язані з прийняттям Закону України “Про забезпечення права на справедливий суд”, даний нормативно-правовий акт є чи не першим кроком на шляху до нормативного закріплення права на справедливий суд у світлі положень міжнародних актів загалом та практики Європейського суду з прав людини зокрема. Реальне подальше втілення досліджуваного права у юридичну практику України не потребує прийняття ще кількох законів. Станом на сьогодні, розвиток права на справедливий суд потребує виконання закріплених у Законі України “Про забезпечення права на справедливий суд” його елементів. Крім того, практику розкриття змісту права на справедливий суд Європейським судом з прав людини повинні вивчати та застосовувати вітчизняні суди таким чином не даючи залишитися такою фундаментальному праву лише закріпленим у законодавстві.

Використана література

1. Про забезпечення права на справедливий суд : Закон України від 12.02.15 р. № 192-VIII ; у ред. від 30.09.16 р. – Режим доступу : http://zakon.rada.gov.ua/laws/show/192-19

2. Ткачук О. Витоки сучасного розуміння права на справедливий суд / Visegrad Journal on Human Rights. – 2016. – № 1/2. – С.188-193.

3. Грень Н. Право на справедливий суд: проблеми незалежності та безсторонності // Вісник Національного університету “Львівська політехніка”. – (Юридичні науки). – 2016. – № 837. – С. 247-251.

4. Загальна декларація прав людини : Резолюція Генеральної Асамблеї ООН № 217 А(III) від 10 грудня 1948 р. // Офіційний вісник України. – 2008. – № 93. – Ст. 89.

5. Міжнародний пакт про громадянські і політичні права : ООН від 16 грудня 1966 р. – Режим доступу: http://zakon3.rada.gov.ua/laws/show /995_043;

6. Про захист прав людини і основоположних свобод : Конвенція Ради Європи від 04 листопада 1950 р. // Офіційний вісник України. – 1998. – № 32. – Ст. 270.

7. Справедливое судебное разбирательство в международном праве : юридический сборник. – Издатель : “Organization for Security and Cooperation in Europe”, 26 сентября 2012 года. – Режим доступу: http://www.osce.org/ru/odihr/100894?download=true

8. Энтин М. Справедливое судебное разбирательство по праву Совета Европы и Европейского Союза // Конституционное право : Восточноевропейское обозрение. – 2003. – № 3(44). – С. 85-97.

9. Афанасьев С.В. Право на справедливое судебное разбирательство : общая характеристика и его реализация в российском гражданском судопроизводстве : монография / С.В. Афанасьев. – Саратов : Научная книга, 2009. – 312 с.

10. Бучик А. Стандарти справедливого суду в розрізі Конвенції про захист прав людини і основоположних свобод / Віче. – 2015. – № 22. – С. 2-5.

11. Case of Golder v. The United Kingdom № 4451/70. URL: http://hudoc.echr.coe.int/eng#{fulltext : CASE%20OF%20GOLDER%20v.%20THE%20UNITED%20KINGDOM], [documentcollectionid2 : “GRANDCHAMBER”, “CHAMBER”], itemid : [001-57496]}

12. Про примусове виконання обов’язку в натурі : Постанова Вищого Господарського суду України у справі № 22/188 за позовом закритого акціонерного товариства “Гефес Інтернейшнл” до приватного акціонерного товариства “Науково-виробниче об'єднання “Агрокомплекс”. – Режим доступу : http://www.reyestr.court.gov.ua/Review/28254300

13. Відшкодування моральної шкоди за створення відповідачем перешкод у використанні права позивача на звернення до суду, про визнання документів письмовими доказами та визнання незаконною бездіяльність відповідача : Додаткове рішення Вінницького районного суду Вінницької області у справі №128/2861/16-ц за позовом ОСОБА_1 до Жмеринського міськрайонного суду Вінницької області. – Режим доступу : http://www.reyestr.court.gov.ua/Review/66663506

14. Case of Salontaji-Drobnjak v. Serbia N 36500/05. URL: http://hudoc.echr.coe.int/eng#{appno : [36500/05], itemid : [001-94985]}

15. Case of Delcourt v. Belgium №2689/65. URL: http://hudoc.echr.coe.int/eng#{fulltext : [Delcourt%20v%20belgium],documentcollectionid2: [“GRANDCHAMBER“, “CHAMBER”], itemid: [001-57467]}

16. Конституція України : Закон України від 28.06.96 р. № 132/94-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

17. Про судоустрій і статус суддів : Закон України від 02.06.16 р. №1402-VIII // Відомості Верховної Ради України (ВВР). – 2016. – № 31. – Ст. 545.

18. Цивільний процесуальний кодекс України : Закон України від 18.03.04 р. № 1618-IV // Відомості Верховної Ради України (ВВР). – 2004. – № 40-41, 42. – Ст. 492.

19. Право на справедливий суд : інші аспекти / Р. Куйбіда, Т. Руда. – (Центр політико-правових реформ; Українська Гельсінська спілка з прав людини). – Режим доступу :https://helsinki.org.ua/pravo-na-spravedlyvyj-sud-inshi-aspekty-r-kujbida-t-ruda-tsentr-polityko-pravovyh-reform

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

До відома читачів

НОВЕ ВИДАННЯ

Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних : збірник документів **;** [неофіційний пер. з англ. І. Майстренко] ; за ред. В. Брижко ; передмова В. Пилипчука. – (Науково-дослідний інститут інформатики і права Національної академії правових наук України). – К. : ТОВ “Видавничий дім “АртЕк”, 2018. – 180 с.

У запропонованому збірнику документів у розвиток опублікованого вченими НДІІП НАПрН України наукового видання **“Становлення і розвиток правових основ та системи захисту персональних даних в Україні”** (див. “Інформація і право”. – № 1(24)/2018. – С. 174) наведено документальні матеріали “Пакету захисту даних” Європейського Союзу, що набули чинності у травні 2018 року.

Видання розраховане на фахівців, експертів і вчених, представників державних і недержавних органів, закладів, установ, підприємств та організацій і має прикладне значення в контексті євроінтеграції України.

Якщо Вас, шановні читачі, зацікавило видання, звертайтеся за адресою:

01032, м. Київ, вул. Саксаганського, 110-В. Науково-дослідний інститут інформатики і права Національної академії правових наук України. Тел.: 234-94-56

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

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 науково обґрунтовувати вирішення визначених автором завдань згідно з такими основними напрямами досліджень, як:
інформаційне право; правова інформатика, інформаційна і національна безпека.

Вимоги до оформлення

1) **Статтю слід подавати українською мовою, виготовлену у друкарський спосіб, та її електронну версію** (структура та зміст якої повністю відповідають друкованому варіанту) у вигляді файлу:
   – *у редакторі Word, шрифт – Times New Roman, з розширенням .doc, кегль – 13;*
   – *параметри сторінки – формат А-4, розташування тексту (таблиці, діаграми тощо) книжне, береги поля (верхній, нижній, лівий і правий краї) – 20 мм;*
   – *відстань між рядками – 1 інтервал;*
   – *кількість матеріалу однієї статті – не більше 15 стор.*

   Стаття має передбачати такі обов’язкові структурні елементи:
   - УДК.
   - Ім’я та прізвище (укр. та англ. мовами), науковий ступінь, вчене звання автора, місце роботи.
   - Назва статті (укр. та англ. мовами).
   - Анотація та ключові слова (укр., англ. та рос. мовами).
   - **Розв’язання проблеми,** шляхом наукового вирішення завдання:
     - **постановка проблеми** *(загальна характеристика)* та **результати аналізу наукових публікацій**, в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття; **наводяться аргументи які підтверджують актуальність і новизну роботи;**
     - **формування мети** *(постановка завдання)* статті;
     - **виклад основного матеріалу** – опис вирішення завдання та обґрунтування наукової цінності та практичного значення визначених у статті результатів.
   - **Висновки** за результатами розв’язання проблеми та вирішення завдання, які визначають наукову новизну роботи. Можуть супроводжуватися пропозиціями, оцінками, гіпотезами, описаними у статті, а також визначенням перспектив подальших досліджень.
   - **Використана література** *(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 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 370 грн. на рахунок Інституту**.

Реквізити для оплати робіт:
Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).

Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

6) Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Вчена рада НДІ інформатики і права НАПрН України не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
  Автори несуть відповідальність за достовірність інформації, що міститься у статтях і повідомленнях до журналу, а також за додержання авторських прав відповідно до законодавства.
- Редакційна колегія залишає за собою право на:

– відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
– внесення до статті змін редакційного змісту у зв’язку з обмеженням обсягу загального матеріалу.

* * * * * * * * * *

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 3(26)/

2018

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.

Founders of magazine:	- Research Institute of informatics and right of National academy of legal sciences of Ukraine; - Vernadsky National Library of Ukraine of National academy of sciences of Ukraine; - Open International University of Human Development “Ukraine”
Publisher:	© Research Institute of informatics and right of National academy of legal sciences of Ukraine.
Address of release:	01032, Kyiv, Saksaganskogo str., 110-V. Research Institute of informatics and right of National academy of legal sciences of Ukraine. Phone.: 234-94-56; e-mail: bvm777@ ukr.net
Web-pages of magazine in the network Internet:	//www.ippi.org.ua – Research Institute of informatics and right of National academy of legal sciences of Ukraine; //www.nbuv.gov.ua – Vernadsky National Library of Ukraine of National academy of sciences of Ukraine.