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

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

Відкритий міжнародний університет розвитку людини "Україна"

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(20)

2017

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

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

м. Київ

УДК 002:340+316.4+338.46:002

* * * * * * * * * * *

З М І С Т

Інформаційне право

Правова інформатика

Інформаційна і національна безпека

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. 12.4. Тираж 100 прим.
Виготовлено з оригінал-макета в друкарні ТОВ “ПанТот” – Свідоцтво про внесення до Державного реєстру видавничої продукції: Серія ДК № 2667 від 25.10.06 р.

Рекомендовано до друку Вченою радою НДІ інформатики і права
Національної академії правових наук України, протокол № 2 від 23.03.17 р.

Інформаційне право

УДК 342.951:001.102 (477)

ЯРЕМЕНКО О.І., *кандидат наук з державного управління, доцент,*
завідувач кафедри правових наук та філософії
Вінницького державного педагогічного університету

ІНФОРМАЦІЙНА СФЕРА ЯК СОЦІАЛЬНО-ПРАВОВЕ ЯВИЩЕ: ПРОБЛЕМИ НАУКОВОЇ ІДЕНТИФІКАЦІЇ ТА РЕГУЛЮВАННЯ

Анотація. *Досліджуються теоретичні засади інформаційної сфери соціуму. Визначено три групи складових інформаційної сфери: суто інформаційну (змістовно-інтелектуальну (контентну) та інфраструктурно-комунікативну), динамічну (інформаційна діяльність та інформаційні відносини), а також складові, які впливають на її стан та розвиток (правова та управлінська). Запропоновано авторське визначення інформаційної сфери.*

Ключові слова:*, соціальні комунікації,спілкування, інформаційна діяльність, інформаційна інфраструкура, інформаційна сфера.*

Аннотация*. Исследуются теоретические основы информационной сферы социума. Определены три группы составляющих информационной сферы: информационную (содержательно-интеллектуальную (контентную) и инфраструктурно-коммуникативную), динамическую (информационная деятельность и информационные отношения), а также составляющие, которые влияют на ее состояние и развитие (правовая и управленческая). Предложено авторское определение информационной сферы.*

Ключевые слова*: социальные коммуникации, общение, информационная деятельность, информационная инфраструкура, информационная сфера.*

Summary. *Theoretical background of information sphere of society is investigated. Three groups of constituents of infosphere are identified: purely informational (content-intellectual (content) and infrastructural-communicative), dynamic (information activities and information relations), as well as constituents, which influence its state and development (legal and administrative). Copyright definition of information sphere is suggested.*

Keywords: *social skills, communication, information activity, information infrastructure, information sphere.*

Постановка проблеми. Однією із визначальних рис сучасності є високий попит соціальних суб’єктів на інформацію та продукти з інтелектуально-інформаційною природою. Як наслідок, поряд з традиційними сферами суспільної життєдіяльності, дедалі більшого значення набуває сфера інформаційна, що актуалізує наукові дослідження в цьому напрямку. Як зазначає Пилипчук В.Г., історичний аналіз свідчить, що інформаційна сфера існувала від часу виникнення людства та суспільних відносин, однак окремі аспекти дослідження інформаційних відносин розпочалися тільки в 60-х роках 20-го століття [1, с. 16].

Інформація та соціальні явища, пов’язані з нею, є предметом вивчення багатьох суспільних наук, в тому числі юридичної, що призвело до появи нової галузі наукового пізнання – інформаційного права. Арістова О.В. підкреслює, що у процесі становлення науки “інформаційне право” спостерігається тенденція накопичення нових наукових даних та розвитку наукових теорій, що може спричинити появу нових ознак та властивостей,

що, у свою чергу, коригує зміст поняття (наприклад, поняття “інформаційне суспільство”, “інформаційна сфера”, “інформаційні відносини”, “інформаційні правовідносини”). Тобто, зазначені поняття є прикладами “понять, що розвиваються” [2, с. 107].

Ряд теоретичних та практичних аспектів інформаційної сфери досліджуються в працях О.В. Арістової., І.Л. Бачило, О.А. Баранова, К.І. Бєлякова, В.М. Брижка, Д.В. Дубова, В.А. Копилова, О.В. Копана, В.К. Конах, Б.А. Кормича, В.Г. Король, О.В. Кохановської, Г.В. Любовець, В.Ф. Попондопуло, Н.А. Савінової, О.В. Сосніна, Т.О. Чернадчук, В.М. Фурашева та інших. В той же час, ця проблематика залишається дискусійною і потребує подальшого науково-теоретичного аналізу.

Метою статті є розкриття соціально-правового змісту поняття “інформаційна сфера”, а також аналіз її складових.

Виклад основного матеріалу. Аналіз вітчизняних та зарубіжних наукових доробок свідчить про те, термін “інформаційна сфера” трактується науковцями з різних позицій, а в основу його дефініцій покладено різні критерії.

Арістова О.В. пропонує визначення національної інформаційної сфери як єдиного інформаційного простору України, який формується суспільством та державою і інтегрується до єдиного Європейського інформаційного простору з урахуванням національної інформаційної безпеки. При цьому під інформаційним простором розуміється соціальне середовище, у якому здійснюється виробництво, збирання, зберігання, поширення і використання інформації, на яке розповсюджується юрисдикція України [3, с. 11]. Водночас, Любовець Г.В. та Король В.Г. ідентифікують сучасний інформаційний простір як певне високодинамічне комунікаційне середовище, яке функціонує за принципом превалювання цілодобових горизонтальних зв’язків, має практично необмежену джерельну базу й потужний взаємодоповнюваний вплив на учасників комунікаційного процесу [4, с. 12].

Баранов О.А. визначає інформаційну сферу як сукупність інформації та інформаційних ресурсів, інформаційної інфраструктури, суб’єктів, що здійснюють оборот інформації, тобто її створення, поширення (передавання), зберігання, використання та знищення, та забезпечують цей оборот, суспільних відносин, які при цьому виникають, системи її правового забезпечення, а також інституційної системи державного управління та регулювання цією сферою [5, с. 21-22].

Бачило І.Л. розглядає інформаційну сферу як об’єктивно виражений стан знань людства про навколишній і створюваний ним у процесі своєї історії світ, що дає змогу користуватися цими знаннями в процесі життя соціуму планети, розвитку земної цивілізації [6, с. 20].

Копилов В.А. визначає інформаційну сферу суспільства як сферу правового регулювання відносин, яка складається з сукупності суб’єктів права, що здійснюють на основі інформаційного та іншого законодавства таку діяльність, що дозволяє вирішувати конкретні інформаційні задачі в суспільстві, включаючи і сам механізм правового регулювання цієї сфери [7, с. 26].

Бєляков К.І. трактує інформаційну сферу як сукупність інформаційних ресурсів в єдності із засобами, методами та умовами, які дозволяють їх активізувати та активно використовувати [8, с. 116]. Автор вважає, що проблеми інформаційної сфери сучасного суспільства можна розглядати, як мінімум, у п’яти аспектах, а саме: адміністративному, правовому, соціальному, економічному і технічному [9, с. 8].

Чернадчук Т.О. пропонує підхід до інформаційної сфери як структурно упорядкованої за змістовними ознаками відносно стійкої сукупності об’єктивно взаємопов’язаних, взаємозумовлених та взаємозалежних елементів (інформаційні

ресурси, інформаційно-телекомунікаційний простір, інформаційне законодавство, системи забезпечення інформаційної сфери), зумовлених закономірностями виникнення, тенденціями розвитку та функціональною залежністю й призначенням [10, с. 261].

Кожен з цих підходів містить в собі сутнісні характеристики інформаційної сфери і є раціональним для розуміння її соціальної та правової природи. В той же час, вважаємо, що виходячи із високого рівня складності інформаційних процесів, здійснити наукову ідентифікацію інформаційної сфери за допомогою однієї дефініції надзвичайно складно. Більше того, на думку Савінової Н.А., категорія “інформаційна сфера” є не надто вдалим визначенням інституціональних утворень держави, на які покладається розвиток та убезпечення комунікацій та відносин, що здійснюються за їх посередництва в умовах розвитку інформаційного суспільства, оскільки, насамперед, термін “сфера” надто вузький для вираження особливостей відносин, які відбуваються в інших сферах (економічних, соціальних, політичних, міжособистісних тощо) [11, с. 63].

Наукову ідентифікацію поняття “інформаційна сфера” ускладнює також те, що для позначення окремих видів інформаційних відносин та процесів науковцями застосовуються такі поняття як “соціокомунікативна сфера”, “сфера інформації”, “сфера інформаційної діяльності”, “сфера права на інформацію”, “сфера інформаційних технологій”, “бібліотечно-інформаційна сфера”, “сфера інформатизації”, “сфера інформаційного забезпечення”, “телекомунікаційна сфера” тощо. У зв’язку з такою термінологічною поліваріантністю, раціональним і обґрунтованим є введення Арістовою О.В. і Чернадчук Т.О. у науковий обіг поняття “інтегративна інформаційна сфера”, яка за інформаційним критерієм (тобто за циркуляцією інформації) об’єднує усі сфери суспільного життя, у тому числі й інформаційну. При цьому інформаційну сферу суспільного життя пропонується розглядати її як сферу, в якій здійснюється суто інформаційна діяльність (збирання, виробництво, зберігання, використання, розповсюдження інформації) та відповідна діяльність, що забезпечує інформаційну діяльність [12, с. 261].

На розвиток цих концепцій та підходів вважаємо за доцільне розрізняти в інформаційній сфері три групи складових: суто інформаційні (змістовно-інтелектуальну (контентну) та інфраструктурно-комунікативну), динамічні (інформаційну діяльність та інформаційні відносини), а також складові, які впливають на її стан та розвиток (правову та управлінську).

Із змістовно-інтелектуальної точки зору, інформаційна сфера – це систематизована та стихійна сукупність інформації у формі баз даних, відомостей, знань, ідей, прогнозів, ресурсів, систем, творів, уявлень тощо, яка перебуває в стані динаміки та постійно збільшується в обсязі, і в якій ідеально відображається минула, теперішня та майбутня соціоприродна об’єктивна та суб’єктивна реальність. На нашу думку, саме таке формулювання відображає інтегративну сутність інформаційної сфери, оскільки, в соціальному обігу одночасно перебуває величезна кількість інформації, що стосується всіх аспектів соціального буття – економічної, політичної, правової, культурної, побутової, особистої тощо. Тобто, в даному випадку, інформаційна сфера розглядається як система глобального відображення всіх інших сфер життєдіяльності суспільства, держави, корпорацій та окремих індивідуумів. Як слушно зазначає Брижко В.М., у наш час життєдіяльність світової цивілізації дедалі більше спрямовується інформаційною сферою, яка завдяки інформаційно-технологічним змінам, що почалися наприкінці XX століття, об’єктивно зумовили появу нового типу суспільства – інформаційного суспільства [13, с. 20]. При цьому особливістю контенту інформаційної сфери нового суспільства є те, що в ньому співвідношення

відображення об’єктивної та суб’єктивної реальності змінюється на користь останньої, за рахунок можливостей маніпулювання інформаційними потоками, дезінформацією, пропагандою, недобросовісною рекламою тощо.

Наявність другої складової інформаційної сфери – комунікативно-інфраструктурної – обумовлюється тим, що обмін інформацією є однією із ключових форм існування соціуму. В свій час, Тофлер Е. вважав, що саме комунікація становить основу інформаційної сфери. Він зазначав, що кожній цивілізації притаманна інфосфера – комунікаційні канали, за допомогою яких поширюється необхідна інформація [14, с. 27].

Соснін О.В., аналізуючи генезис інформаційної сфери, зауважує, що подолавши за допомогою засобів обчислювальної техніки два гальма на шляху свого розвитку – швидкість і обсяги передачі інформації, технології зв’язку, починаючи з часів появи телеграфу (1847 р.), темпами свого розвитку стали багато в чому визначати процеси розвитку людства і загострення конкуренції на світових ринках, утворивши інформаційну сферу сукупністю великої різноманітності інформації й інформаційної інфраструктури суспільства. Їй притаманна своя форма суспільних відносин, об’єктом яких є інформація як ресурс й інформаційна інфраструктура [15, с. 263].

Таким чином, інформаційну сферу як інфраструктурно-комунікативне явище можна розглядати як сукупність суб’єктів інформаційної та інфраструктурної (комунікаційної) діяльності, які з використанням інформаційних технологій та технічних засобів забезпечують приватне спілкування та публічні комунікації, а також суспільний обіг як власної інформації, так і інформації, що знаходиться у володінні, користуванні та розпорядженні інших суб’єктів, а також її зберігання, обробку, знищення, захист та охорону.

На нашу думку, в сучасних умовах комунікативна складова інформаційної сфери значною мірою є похідною від контентної, оскільки саме наявність значних обсягів інформації, що циркулює в суспільстві, а також високий соціальний попит на неї мотивують інституалізацію особливого виду діяльності – комунікаційно-інформаційної. Як підкреслює Савінова Н.А., інформація є складовою комунікації і не має самостійної здатності передаватися від комунікатора до реципієнта без наявності дієвої структури комунікації, у якій інформація виступає лише предметом передавання, хоча і змістовним [16, с. 43].

В інформаційному суспільстві, поряд з традиційним міжособистісним спілкуванням, значного поширення набувають саме соціальні комунікації, які розглядаються як різновид комунікації, що реалізується на рівні суспільства за допомогою спеціально організованих соціальних інститутів, установ, закладів, організацій тощо, призначенням яких є створення та передавання в часі та просторі соціально значущої інформації в документально фіксованому або усному вигляді [17, с. 5].

На думку Ільганаєвої В., глобальність та єдність інформаційної взаємодії в суспільстві забезпечується у будь-якій формі фіксації, збереження, опрацювання, збирання, розповсюдження та використання інформації як продукту духовної практики людства. Ці процеси забезпечують відповідні соціально-комунікативні структури, які також виконують окремі завдання в системі суспільної взаємодії, – бібліотеки, архіви, преса, музеї, радіо, ТБ, центри інформації та документації. Усі діючі соціально-комунікативні структури здійснюють притаманні сфері обігу соціальної інформації процеси та операції, що мають свої особливості, пов’язані з окремими процесами в часовому (засоби фіксації інформації, канали її розповсюдження) або просторовому (ЗМІ, архіви, музеї, бібліотеки, інформаційні системи) вимірі [18, с. 263].

Слід зазначити, що змістовно-інтелектуальна та інфраструктурно-комунікативна складові інформаційної сфери тісно пов’язані між собою і здійснюють взаємовплив на різних рівнях, особливо суб’єктно-функціональному. Так, ряд суб’єктів інформаційної діяльності є творцями інформаційних продуктів тобто поповнюють контентну частину інформаційної сфери і, водночас, здійснюють їх поширення. Цей зв’язок проявляється також і в комплексній сутності багатьох видів професійної інформаційної діяльності. В сучасних умовах навіть інституції, які традиційно тільки зберігали носії інформації для суспільного та приватного користування – архіви, бібліотеки, музеї, під впливом збільшення обсягів інформації та розвитку технічних засобів комунікації впроваджують в свою діяльність інформаційно-комп’ютерні технології і стають активними учасниками інформаційних та інформаційно-комунікаційних відносин.

Особливо слід підкреслити нероздільність змістовно-інтелектуальної та інфраструктурно-комунікативної складової інформаційної сфери у віртуальній реальності, яка стає домінуючою в інформаційних процесах і акумулює великі обсяги інформації, а також є потужним засобом соціальних комунікацій. Створене інформаційно-комунікаційними технологіями “віртуальне” середовище є не якоюсь альтернативою, а невід’ємною частиною реального світу, що знайшло свій вираз у концепції “реальної віртуальності”, комунікація та взаємодія в рамках якої впливає на життя суспільства та держави [19, с. 51].

Здійснивши синтез цих двох складових, інформаційну сферу можна трактувати як глобальне системоутворююче явище життєдіяльності суспільства та держави, що складається із сукупності впорядкованої та стихійної соціоприродної інформації, а також системи індивідуумів та інституцій, які забезпечують її обіг, соціальні комунікації та спілкування.

Практичне функціонування інформаційної сфери, її соціальна динаміка здійснюється в процесі інформаційної діяльності та інформаційних суспільних відносин. Попондопуло В.Ф. наступним чином пов’язує ці дві явища: соціальна діяльність (зміст) опосередковується суспільними відносинами (формою) [20, с. 263]. Такої ж позиції дотримуються вчені в галузі інформаційного права, які, визначаючи основні функціональні напрямки інформаційної діяльності, підкреслюють, що за ними виникають суспільні відносини, які регулюються інформаційним правом, як галуззю юридичної науки, що досліджує правові проблеми в інформаційній сфері [21, с. 763].

Вважаємо, що інформаційну діяльність доцільно розглядати під двома кутами зору: загально-соціальним і вузько-юридичним. Інформаційну діяльність в загально-соціальному розумінні слід трактувати виходячи з того, що суспільство є інтелектуалізованою, високоорганізованою системою з інформаційною взаємодією між його суб’єктами, яка виступає в якості необхідної умови його ефективного функціонування. При цьому, обіг інформації в соціальних підсистемах досить часто є стихійним, а значна група інформаційних процесів є елементом повсякденного життя людини. У зв’язку з цим, певні дії суб’єктів із соціальною інформацією можна кваліфікувати як інформаційну діяльність лише умовно. Інформаційна діяльність у вузько-юридичному розумінні розглядається як система інтелектуальних, творчих, організаційних і технологічних дій та заходів суб’єктів права, які спрямовані на функціонування та розвиток інформаційної сфери, що здійснюються на основі законодавства в рамках суспільного або корпоративного поділу праці [22, с. 70].

Аналогічно, суспільні відносини в інформаційній сфері слід розглядати як такі, що врегульовані правовими нормами, і ті, які знаходяться поза таким регулюванням. Обґрунтованим є узагальнююче трактування суспільних відносин як структурної

сукупності конкретно історичних соціальних зв’язків, залежностей та обмежень, які виникають в процесі і результаті суспільно значимої предметної діяльності і мають властивість постійно повторюватися [23, с. 84]. Інформаційні відносини як суспільне явище, є особливою групою відносин, які мають місце в інтегративній інформаційній сфері в процесі здійснення діяльності, пов’язаної з інформацією. З правової позиції, їх можна трактувати як особливу групу відносин, які виникають, розвиваються і припиняють свою дію в процесі здійснення різних видів соціальної діяльності щодо створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації, яка регулюється нормами інформаційного права та інших галузей системи національного законодавства, а також міжнародними нормами. Складна юридична природа суспільних відносин в інформаційній сфері передбачає необхідність їх типологізації, тобто виділення із загального масиву цих відносин окремих складових, об’єднаних типовими характеристиками. На цій основі можна виокремити інформаційні правові відносини, інформаційно-інфраструктурні, інформаційно-процедурні та інформаційно-процесуальні правові відносини [24, с. 263].

Таким чином, можна стверджувати, що більшість відносин в інформаційній сфері носять правовий характер і врегульовані правом або об’єктивно цього потребують. Визначальну роль права в регулюванні інформаційної сфери підкреслюють і науковці в галузі соціології, які зазначають, що соціально-правові відносини формуються у результаті спільної практично-перетворювальної діяльності людей, становлять фундамент формальної структури будь-якого соціального інституту в суспільстві та підтримують систему санкцій стосовно виконання його соціальними суб’єктами своїх функцій. Ці форми відносин існують та відтворюються виключно на основі консенсусно визначеної й унормованої системі правил, норм і цінностей, тобто переважно на праві. Отже, соціально-правові відносини є базовою складовою соціального механізму правової системи, справляючи регулятивний вплив на суспільні відносини [25, с. 11].

Для позначення процесів правового впливу на інформаційну сферу науковцями застосовуються різноманітні юридичні конструкції – “впорядкування інформаційних відносин” (Брижко В.М.), “правове забезпечення інформаційної сфери” (Баранов О.А), “законодавча регламентація інформаційних відносин” (Лопатін С.І.) тощо.

Слід відзначити, що взаємозв’язок інформаційної сфери і права характеризується високим рівнем складності. Системоутворююча сутність інформаційної сфери проявляється в тому, що вся багатоманітність і складність соціальних взаємодій, впливів, зв’язків, конфліктів, процесів проявляється через інформаційні суспільні відносини. Право, регулюючи ці відносини, водночас саме по собі теж є інформаційною системою, відповідно, воно знаходиться в двох вимірах – правовій та інформаційній сферах. Правові норми, що регулюють відносини в інформаційній сфері, є складовою системи законодавства, яку ще називають законодавчою сферою. Таким чином, сфера законодавства “накладається” на інформаційну сферу в частині суспільних відносин врегульованих нормативно. При цьому однією із проблем впливу права на інформаційну сферу є визначення тих інформаційних відносин, які потребують першочергового законодавчого врегулювання. Фахівці в галузі інформаційного права підкреслюють, що суспільні відносини в інформаційній сфері потребують правового регулювання тоді, коли їх предметом виступають суспільно значимі процеси, пов’язані з обігом та використанням інформації, а суб’єкти правовідносин мають взаємні права і обов’язки, гарантовані державою [26, с. 11].

В цьому аспекті доцільним є використання міжнародного досвіду, зокрема, Європейського Союзу. Так, керівні документи, що регулюють інформаційну сферу в ЄС, можна умовно розділити на чотири основні напрями: розвиток інформаційного суспільства (розроблення та використання новітніх інформаційно-комп’ютерних технологій та упровадження заснованих на них форм діяльності – е-уряд, е-банкінг, е-документообіг тощо); розвиток офіційної комунікативної діяльності (інформування громадськості про процеси в ЄС, формування позитивного іміджу ЄС тощо) і “стратегічних комунікацій”; забезпечення інформаційної безпеки країн ЄС та їхніх громадян (захист інформаційного суверенітету, забезпечення інформаційних прав та свобод громадян, визначення режимів функціонування інформації тощо); розвиток спільного європейського медіа-простору (питання, пов’язані з діяльністю масмедіа, в тому числі конвергентних медіа, сприяння розвитку кіносфери, підтримки функціонування бібліотек тощо) [27, с. 11].

На основі законодавства функціонує також система державного управління інформаційною сферою та державна інформаційна політика. На сьогодні центральним органом виконавчої влади, який здійснює державне управління в інформаційній сфері є Міністерство інформаційної політики України. Основними його завданнями визначено забезпечення інформаційного суверенітету України, зокрема з питань поширення суспільно важливої інформації в Україні та за її межами, забезпечення функціонування державних інформаційних ресурсів, а також здійснення реформ засобів масової інформації щодо поширення суспільно важливої інформації [28, с. 11]. Вважаємо, що управління інформаційною сферою в рамках цих двох окреслених завдань не відповідає сучасним вимогам інформаційного розвитку. Цілком погоджуємося із Дубовим В.Д., який зазначає, що сьогодні державна інформаційна політика потребує ґрунтовного перегляду, передусім у частині пріоритетів, і виділяє такі її цілі: 1) адаптацію законодавства, що регулює інформаційну сферу та інформаційні відносини, до реалій гібридного протистояння; 2) вироблення нової моделі функціонування медіа-середовища, яке б відповідало чинному етапу розвитку українського суспільства; 3) створення дієвої спеціальної державної інформаційної політики щодо окупованих територій та лінії розмежування; 4) розвиток медіа- та цифрової освіти на всіх рівнях; 5) реформування системи інформаційного позиціонування України на міжнародній арені в напрямі її більшої гнучкості та ефективності; 6) проведення реформи внутрішньої комунікативної діяльності держави та реформи урядових комунікацій; 7) розвиток потенціалу стратегічних комунікацій як механізму протидії деструктивній інформаційній діяльності щодо України [29, с. 92].

Висновки.

Сучасні науковці розглядають інформаційну сферу з різних позицій і акцентують увагу на різних її аспектах. Виходячи з того, що інформаційна сфера є надскладне соціальне явище, наукову ідентифікацію її необхідно здійснювати шляхом аналізу тісно взаємопов’язаних і взаємозалежних її складових: змістовно – інтелектуальної та інфраструктурно-комунікативної, динаміка яких проявляється в інформаційній діяльності та інформаційних відносинах. Здійснивши синтез цих двох складових, інформаційну сферу можна трактувати як глобальне системоутворююче явище життєдіяльності суспільства та держави, що складається із сукупності впорядкованої та стихійної соціоприродної інформації, а також системи індивідуумів та інституцій, які забезпечують її обіг, соціальні комунікації та спілкування.

Стихійність розвитку інформаційної сфери в поєднанні з високим рівнем її соціальної значимості обумовлює необхідність активного впливу на неї держави. Основними інструментами такого впливу є інформаційне законодавство, інформаційна політика та державне управління. Ці чинники, з одного боку, є зовнішніми факторами, що впливають на інформаційну сферу, з іншого, після відповідних процедур їх інституалізації, вони стають частиною інформаційної сфери, в якості її державного регулятора.

Використана література

1. Пилипчук В. Системні проблеми розвитку правової науки в інформаційній сфері // Вісник Академії правових наук України. – 2011. – № 3. – С. 16-27.

2. Арістова І.В. Становлення науки “інформаційне право” : питання методології (частина друга) // Публічне право. – 2016. – № 3. – С. 101-102. – Режим доступу : http://nbuv.gov.ua/JRN/pp_2016_2_35.

3. Арістова І.В. Еволюційний розвиток поняття “інформаційна сфера” // Вісник Національного університету внутрішніх справ. – 2005. – Вип. 31. – С. 239-245.

4. Любовець Г.В., Король В.Г. Аналіз підходів до моніторингу інформаційного простору в Україні // Держава та регіони. – 2015. – № 3. – С. 10-16. – (Серія : Соціальні комунікації).

5. Баранов О.А. Правове забезпечення інформаційної сфери : теорія, методологія і практика : монографія / О.А. Баранов. – К. : Едельвейс, 2014. – 433 с.

6. Бачило И.Л. Информационное право : учебник / И.Л. Бачило, В.Н. Лопатин, М.А. Федотов ; под ред. Б.Н. Топорнина. – СПб. : Юридический центр Пресс, 2001. – 725 с.

7. Копылов В.А. Информационное право : учебник / В.А. Копылов. – М. : Юристъ, 2002. – 512 с.

8. Бєляков К.І. Інформатизація в Україні : проблеми організаційного, правового та наукового забезпечення : монографія / К.І. Бєляков. – К. : КВІЦ, 2008. – 576 с.

9. Беляков К.І. Інформаційно-правові дослідження : походження, становлення, стан та перспективи розвитку // Інформація і право. – 2011. – № 2. – С. 4-12.

10. Чернадчук Т.О. Деякі питання щодо характеристики інформаційної сфери України // Держава і право. – 2011. – Вип. 52. – С. 255-263.

11. Савінова Н.А. Кримінально-правова політика та убезпечення інформаційного суспільства в Україні : монографія / Н.А. Савінова. – К. : Ред. журналу “Право України”. – 2013. – 292 с.

12. Арістова І.В., Чернадчук Т.О Концепція інформаційних правовідносин : сутність та особливості використання у сфері банківської діяльності // Інформація і право. – 2012. – № 3. – С. 47-56.

13. Брижко В.М. Філософія права : герменевтика в сфері інформаційного права // Правова інформатика. – 2014. – № 1. – С. 18-22.

14. Тоффлер Э. На пороге будущего. “Американская модель” : с будущим в конфликте / Э. Тоффлер. – М., 1984.

15. Соснін О.В., Корнейко О.В., Олійник О.В. Проблеми життєдіяльності інформаційної сфери // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2009. – Вип. 20. – С. 261-273.

16. Савінова Н.А. Вади сучасної правової комунікації // Правова інформатика. – 2014. – № 4. – С. 40-48.

17. Шейко В.М., Кушнаренко Н.М. Перспективи розвитку соціальних комунікацій як нової наукової галузі : матеріали Міжнар. наук. конф. [“Соціальні комунікації в стратегіях формування суспільства знань”], (Харків, 26 – 27 лют. 2009 р.) : у 2 ч. / М-во культури і туризму України, Харк. держ. акад. культури, Акад. мистецтв України, Ін-т культурології. – Х., 2009. – Ч. 1. – С. 3-8.

18. Ільганаєва В. Інституціоналізація соціально-комунікаційної сфери суспільства // Освіта регіону. Політологія, психологія, комунікації. – 2008. – № 1/2. – С. 148-153.

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

20. Попондопуло В.Ф. Система общественных отношений и их правовые формы (к вопросу о системе права) // Правоведение. – 2002. – № 4. – С. 78-101.

21. Правова доктрина України : у 5 т. – Т. 2 : Публічно-правова доктрина України / [Ю.П. Битяк, Ю.Г. Барабаш, М.П. Кучерявенко та ін.]. ; за заг. ред. Ю.П. Битяка. – Х. : Право, 2013. – 864 с.

22. Яременко О.І. Сутність та соціально-правова природа інформаційної діяльності // Інформація і право. – 2013. – № 3. – С. 65-73.

23. Ткаченко Ю.Г. Методологические вопросы теории правоотношений / Ю.Г Ткаченко. – М. : Юрид. лит., 1980. – 176 с.

24. Яременко О.І. Теоретико-методологічні підходи до юридичної природи інформаційних відносин та їх типологізація // Інформація і право. – 2016. – № 4. – С. 13-21.

25. Огаренко Т.О. Соціальні фактори регулювання правової системи : проблемне поле дослідження // Держава та регіони. – 2013. – № 2. – С. 28-32. – (Серія : Право).

26. Фурашев В.М Систематизація і розвиток теоретичних основ трансформації інформаційних відносин на шляху до кіберцивілізації : наук. доп. / В.М. Фурашев, С.Ю. Петряєв, В.М. Поперечнюк. – К. : ФСП НТУУ “КПІ”, 2016. – 55 с.

27. Конах В.К. Система концептуальних документів ЄС в інформаційній сфері як приклад для України / Стратегічні пріоритети. – 2016 . – № 3 (40). – С. 93-93.

28. Питання діяльності Міністерства інформаційної політики України : Постанова Кабінету Міністрів України від 14.01.15 р. № 2. – Режим доступу : http://zakon3.rada.gov.ua/laws /show/2-2015-%D0%BF

29. Дубов Д.В. Державна інформаційна політика України в умовах гібридного миру та війни : стратегічні пріоритети / Стратегічні пріоритети. – 2016. – № 3 (40). – С. 84-93.

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

УДК 342.951:351/354

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

КОМУНІКАЦІЯ ВЛАДИ І СУСПІЛЬСТВА В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ[*]

Анотація. *В даній статті досліджується питання сутності, сучасного стану, проблеми, основні механізми та форми взаємодії держави і суспільства. Розглядаються підходи до функціонування органів державної влади в умовах модернізації та суспільних трансформацій. Досліджується роль громадянського суспільства на сучасному етапі у процесі вироблення та формування публічної політики, роль держави у формуванні та розвитку громадянського суспільства.*

Ключові слова: *влада, Інтернет, інформація, комунікація, реформування, суспільство.*

Аннотация. *В данной статье исследуется вопрос о сущности, современном состоянии, проблемах, основных механизмах и формах взаимодействия государства и общества. Рассматриваются подходы к функционированию органов государственной власти в условиях ее модернизации и общественных трансформаций. Исследуется роль гражданского общества на современном этапе в процессе разработки и формирования публичной политики, роль государства в формировании и развитии гражданского общества.*

Ключевые слова: *власть, Интернет, информация, коммуникация, реформирование, общество.*

Summary. *This article explores the question of essence, the present state, problems, basic mechanisms and forms of cooperation between the state and society; the approaches to the functioning of public authorities in terms of its modernization and social transformation. We investigate the role of civil society at the present stage in the process of the development and formation of public policy, the state's role in the formation and development of civil society.*

Keywords: *authority, Internet, information, communication, reforming, society.*

Постановка проблеми. Взаємодія влади і структур громадянського суспільства постійно набуває політичної гостроти та зростаючої актуальності. Актуальність зазначеного обумовлено тим, що в демократичній державі влада не може ефективно функціонувати без взаєморозуміння і конструктивної взаємодії з громадянським суспільством, яке являє собою множинність самодіяльних, незалежних від держави соціальних груп та індивідів, які самостійно захищають свої інтереси.

Демократизація політичного життя, децентралізація влади, здійснювані реформи у державі відбуваються в умовах ускладнення простору політичної комунікації та урізноманітнення технологій комунікативної взаємодії. При збільшенні кількості суб’єктів політичного процесу зростає і якість їх взаємозв’язку, що пов’язано як з диверсифікацією джерел інформації, так і з удосконаленням технічного забезпечення влади і громадян. Особливого значення в цих умовах набуває готовність і здатність органів державної влади та місцевого самоврядування використовувати ефективні механізми взаємодії з громадськістю, як безпосередньо (з залученням громадських організації), так і опосередковано (через мас-медіа). В умовах здійснюваних реформ

[*] Робота є продовженням досліджень за темою НДР “Науково-методичне, правове та інформаційне забезпечення формування національної інтегрованої системи нормативно-правових актів в умовах децентралізації в Україні”.

в Україні, можна констатувати, що комунікативні технології у сфері взаємовідносин гілок влади і суспільства активно використовуються усіма політичними гравцями. Однак часто зазначене посилює конфронтацію між ними. Тому є необхідним напрацювання механізмів та форм налагодження взаєморозуміння між усіма суб’єктами відносин.

Вплив комунікативних технологій на суспільні відносини постійно знаходиться у полі зору вітчизняних дослідників. Певну увагу зазначеному приділяли такі науковці, як: І. Арістова, О. Баранов, К. Бєляков, В. Брижко, О. Довгань, В. Гура, О. Золотар, Л. Климанська, М. Кравчук, А. Марущак, В. Настюк, В. Пилипчук, Г. Почепцов, Н. Савінова, В. Фурашев, В. Шкляр, Д. Яковлев та інші.

Метою статті є здійснення аналізу стану взаємодії влади і суспільства, визначення існуючих проблем, ролі влади і громадськості у виробленні та реалізації публічної політики держави у сучасних умовах.

Виклад основного матеріалу. Нині в Україні провадиться ряд реформ, які кардинально мають змінити суспільне життя в державі, прискорити подальший поступ країни у всебічному її розвитку. Це є своєрідною довгоочікуваною відповіддю на суспільний запит щодо зміни існуючої системи влади в Україні. Відповідні спроби її зберегти чи завадити її реформуванню шляхом адаптації її до сучасних умов є одною із загроз національному суверенітету та державності. Нині взаємини між так званим «центром» і регіонами характеризується хитким балансом доцентрових і відцентрових напрямків, що створює загрозу виникнення конфлікту між ними.

Відповідно до базових документів держави [1 – 4], їхніми положеннями передбачається проведення у державі 62 реформи, 18 з яких є ключовими, такі як: реформування місцевого самоврядування, децентралізація державної влади тощо.

Як зазначав на нараді “Основні напрямки децентралізації влади в Україні в 2016 році” [5] Прем’єр-міністр України В. Гройсман, одним із перших кроків здійснюваних реформ має бути підтримка з боку державної влади об’єднання громад, їх укріплення, що дозволить значно підвищити їхню всебічну спроможність, а також передача повноважень місцевому самоврядуванню і розвиток місцевої демократії. Механізм місцевої демократії, можливості впливу громадян на свою владу має залишатися в полі нашої уваги і прийняття конкретних рішень. Вирішення цього питання здатне забезпечити відповідальність органів місцевої влади як перед державою, так і перед громадою. Таким чином спроможність, повноваження і відповідальність, розвиток місцевої демократії – три ключові завдання що дозволять змінити ситуацію в державі у кращий бік.

Зазначене передбачає істотну зміну режиму комунікації між органами влади – як центральними, так і на місцевому рівні – з громадянами зокрема, та з громадянським суспільством в цілому, і передбачає виникнення нагальної потреби у проведенні постійного переговорного процесу влади і громадянського суспільства, окремих громадян, представників малого і середнього бізнесу.

Необхідно зазначити, що на сьогоднішній день існують різні форми, засоби та види комунікації влади і суспільства. Широкого вжитку нині набули саме засоби масової комунікації. Якщо раніше комунікації між владою та населенням полягали в особистому спілкуванні представників влади і населення, то сучасний етап розвитку технологій призвів до появи особливого виду масової комунікації – від друкованих засобів і електронних засобів (телебачення, радіо) комунікації, до Інтернет-комунікацій, які характеризуються високою швидкістю передавання та поширення інформації. Застосування Інтернет-комунікацій (інформаційно-комунікаційних систем – ІКС) дозволяє утримувати великий обсяг інформації і сприяти розвитку громадянського

суспільства. Процес Інтернет-комунікації підживлює формування ефективного діалогу між владою і суспільством, дозволяє здійснювати взаємодію представників влади безпосередньо з цільовою аудиторією і тим самим отримувати зворотну реакцію.

ІКС являють собою свого роду інформаційну базу, в якій акумулюється, зберігається і відтворюється безмежний об’єм інформації, що, у свою чергу, забезпечує оперативний доступ до неї. Крім того, ІКС відіграє важливу роль у розвитку громадянського суспільства щодо розширення функції соціального контролю влади. Також спрощується і зворотній процес – формування суспільної думки [6].

Необхідно зазначити, що дослідники, які ведуть наукову розвідку сучасних засобів масової інформації, включаючи використання соціальних мереж, відзначають, що сьогодні віртуальне спілкування шляхом використання Інтернет отримало велику популярність у населення, що підтверджується різними дослідженнями користувачів мережі Інтернет і соціальних мереж. В Україні кількість користувачів мережі Інтернет зростає швидкими темпами. Якщо 20 років тому лише 1 % українців користувалися мережею Інтернет, то зараз – 62 %. За останні два роки кількість користувачів зросла на 8 відсоткових пунктів, йдеться на порталі ZN.UA (див. Рис.) [7].

Частка користувачів серед людей 18 – 39 років в Україні сягнула 91 %, свідчать дані опитування КМІС. Як зазначають соціологи, кількість користувачів Інтернету продовжує зростати більшими темпами, ніж це прогнозувалося і суттєво варіюється в залежності від області проживання. Найбільш домогосподарств із домашнім підключенням спостерігається у Києві (78 %), найменше – у Кіровоградській області майже в 2,5 разів менше. Однак, згідно з опитуванням КМІС, проведеним у жовтні 2014 року, телебачення залишається основним джерелом отримання новин для переважної більшості українців: 83,5 % респондентів вказали, що джерелом виступає українське телебачення, 31 % – Інтернет-сайти, 29 % – знайомі і родичі.

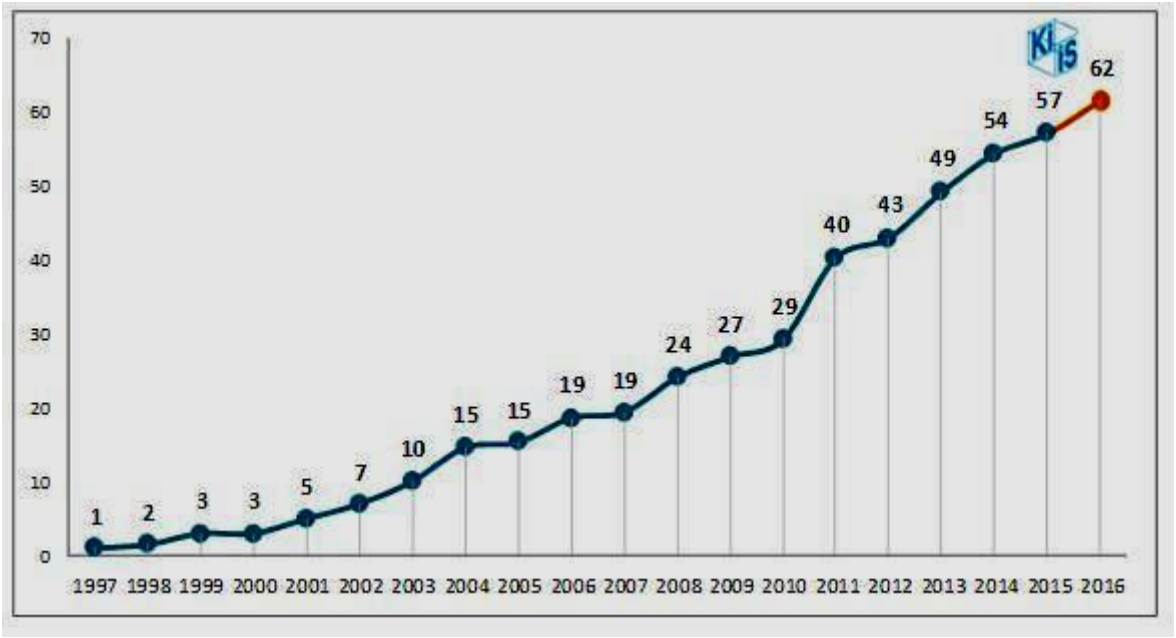

Рис.

Таким чином, Інтернет-комунікації можуть сприяти розвитку взаємодії як між людьми, так і між органами державної влади і населенням, стати важливим засобом зворотного зв’язку. Нині виборчий штаб будь-якого кандидата в депутати, органи влади використовують сучасні інформаційні технології для здійснення моніторингу

коментарів і публікацій громадян і виборців, виокремлюючи найбільш важливі і значні питання і проблеми коментаторів. Навколо блогів, спільнот і форумів популярних політиків, партій, громадських чи державних представників утворюється велика кількість учасників, які обговорюють важливі питання щодо різних тем, які пов’язані із соціально-політичними процесами. Дуже часто класичні і цифрові ЗМІ включаються у зазначене спілкування за допомоги надання можливостей на своїх майданчиках обговорювати різноманітні питання. Вони створюють свої аналоги на просторах Інтернет і тим самим підвищують свою популярність і рівень довіри населення до них.

Присутність політика чи державного чиновника у соціальних мережах робить його таким самим, як і усі інші користувачі: наявність можливих друзів, партнерів, опонентів, можливість написати повідомлення чи коментар, його хобі чи повсякденні заняття тощо. Таким чином вони стають більш доступними для громадськості, що може вплинути на думку людей щодо їхньої відкритості і доступності, сприяє більшій довірі до нього з боку суспільства, ніж на офіційних зустрічах і передачах.

Необхідно зазначити, що проблема дослідження взаємодії влади і суспільства була завжди актуальною, оскільки полягає у складності інформування усього населення про діяльність влади, а також в отриманні зворотного зв’язку від населення щодо проблем, які існують у суспільстві. З появою класичних ЗМІ дана проблема була частково вирішена. З появою мережі Інтернет, органи влади створили свої представництва у вигляді Інтернет-порталів, що сприяло зближенню з народом, а також сформувалась думка про те, що органи влади мають бути відкритими і доступними суспільству.

У процесі функціонування органів державної влади, коли інформаційний супровід їх діяльності не завжди є відкритим, питання зворотного зв’язку між владою і суспільством набуло актуальності, що і стало одною із підстав для реформ, здійснюваних нині в Україні. В соціальних мережах представники громадськості відкрито висловлюють свою позицію, формуючи суспільну думку про недостатню відкритість діяльності органів державної влади та місцевого самоврядування, про імітацію ними здійснення комунікації з населенням. Зазначене потребує від органів влади підвищення своєї відкритості і легітимності, а також оперативного здійснення комунікації з суспільством для вирішення проблем, що виникають у суспільстві.

Враховуючи те, що аудиторію більшості популярних соціальних мереж складає молодь, існує доцільність використання цих мереж для комунікації саме з активною молоддю, яка спроможна формувати громадську думку. Зазначене є важливим, оскільки комунікації шляхом використання соціальних мереж може позитивно відобразитись на іміджі та авторитеті влади, на формуванні у суспільстві позитивної думки щодо відкритості і доступності влади для людей. Крім того, витрати на комунікацію шляхом використання соціальних мереж Інтернету можуть бути менш затратними, ніж інформування громадськості про діяльність влади на різних інформаційних ресурсах.

Таким чином, ефективна комунікація – це взаємодія, що передбачає зворотній зв’язок та дозволяє підтримувати інтерес і довіру населення до діяльності влади. Вона спрямована на формування довготривалого лояльного відношення до законодавчої та виконавчої влади, органів місцевого самоврядування. Як зазначають експерти, важливість формування ефективної комунікації доцільна з наступних причин:

– ефективна комунікація між владою і населенням сприяє вирішенню проблем громадян шляхом донесення їх до влади;

– вирішуючи проблеми громадян, влада формує про свою діяльність позитивну думку, тим самим сприяє підвищенню рівня довіри і мінімізує можливі протести з боку суспільства;

– висвітлюючи таку діяльність, ЗМІ підвищують і свій рейтинг, шляхом підвищення кількості переглядів реальними людьми і подіями, учасники яких цікавляться даними сюжетами.

Зазначений взаємозв’язок вигідний для обох сторін, оскільки кожна з них отримує наступні позитивні преференції:

– можливість швидкого доведення інформації до населення про важливі події, не задіюючи для зазначеного журналістів;

– можливість посилення своєї позиції у політиці в рамках проведення відповідної інформаційної політики;

– використання та оперування думкою своїх експертів, тим самим зміцнюючи їхній авторитет і формуючи думку у суспільстві про професіоналізм зазначених осіб [8].

Для населення ж зазначене надає можливість отримати інформацію про важливі події із першоджерела та відповідних експертів, незалежно від часу доби, а також мати можливість прокоментувати їх чи задати питання безпосередньо авторам повідомлення, тим самим розвиваючи мережеву комунікацію. Одночасно, така палітра думок, таке існування плюралізму думок, що являє собою свободу виразу політичних поглядів, однозначно сприятиме розвитку громадянського суспільства.

На думку багатьох дослідників, найбільш оптимальним механізмом комунікації для влади є соціальні мережі. Однак при їх використанні акцент має бути зосереджений не на простому інформуванні громадян про розвиток подій, а на роз’ясненні прийнятих рішень, що мають суспільний інтерес і суспільне значення, а також на отриманні від громадян наказів, пропозицій щодо вирішення тих чи інших важливих проблемних питань. Крім того, використання соціальних мереж буде набагато доцільніше і логічніше, якщо зазначене буде здійснюватися від імені конкретних осіб (політиків, посадових осіб тощо) з метою виконання адміністративних і політичних рішень.

У сучасній демократичній державі, в якій інститути громадянського суспільства функціонують достатньо ефективно, державно-владні структури не можуть встановлювати так звані “власні правила гри” у відносинах з громадськістю, оскільки в такому разі будь-які рішення, навіть досить ефективні і такі, що відповідають інтересам громадськості, не будуть мати легітимності. Основним критерієм ефективності функціонування відносин влади з громадськістю є створення умов для вільного схвалення громадянами дій органів влади, прийнятих ними рішень. Тому саме у формі двостороннього, збалансованого зв’язку суспільства та влади створюються найбільш оптимальні умови для ефективного функціонування суб’єктів зазначених відносин оскільки передбачає:

– відкритість інформаційних потоків у поясненні змісту державної політики, що гарантує максимальну свободу в обговоренні суспільних проблем;

– сприяння розумінню громадянами діяльності органів державної влади, доцільності прийняття ними відповідних рішень;

– активну участь громадськості в управлінні державою, яка супроводжується систематичним залученням її до вирішення соціально значущих проблем;

– організацію та підтримку владою соціальних дискусій шляхом залучення громадськості до процесів творення та реалізації державної політики [9, с. 11].

Реалізація зазначеного підвищує інтерес до потенціалу нових форм державного управління, які запроваджені в демократичних країнах, сприяє оновленню суспільних відносин під впливом орієнтації на діалог, свободу і активну участь громадськості в державному управлінні, демократизації соціальних інститутів, налагодженню діалогових форм співпраці влади та громадськості України.

Як зазначено в науковій літературі, важливим елементом діалогу влади і громадськості є консультації через такі засоби, як різні форми опитування, громадські слухання, симпозіуми, конференції, “гарячі лінії”, за допомогою інформаційних технологій тощо, що є формою залучення громадян до участі у процесі ухвалення рішень, що на них впливають. Так, під публічними консультаціями розуміють процес комунікації між органами державної влади та громадянами (зацікавленими сторонами), за допомогою якого обидві сторони отримують інформацію про різні перспективи та пропозиції парламентської законотворчої чи урядової політики, які надають можливість громадянам впливати на зміст рішень, що ухвалюються органами державної влади.

Для Уряду консультації є засобом:

– збирання інформації, потрібної для вироблення публічної політики;

– більшого залучення громадян до розгляду питань, які безпосередньо або опосередковано їх стосуються;

– залучення різноманітних позаурядових груп (зацікавлених сторін) до процесу формування та впровадження державної політики;

– вимірювання впливу (зокрема рівня задоволення) владних рішень на зацікавлені сторони;

– отримання пропозицій до дискусійних і складних рішень, які зачіпатимуть економічні, соціальні чи політичні інтереси окремих громадян чи груп людей більше, ніж інших;

– досягнення підтримки громадян для прийняття пропонованого рішення;

– поліпшення якості процесу вироблення політики;

– визначення пріоритетів, потреб і застережень зацікавлених сторін;

– підвищення рівня обізнаності громадян про державні справи;

– сприяння обміну думками, поглядами та інформацією.

Консультації є інструментом громадян стосовно:

– поліпшення якості публічної політики;

– участі в демократичному управлінні державою;

– розуміння та підтримки владних рішень, здійснення публічного контролю за їх реалізацією. Публічні консультації – це стратегія, вироблена для залучення широкої громадськості та встановлення суспільної довіри до політики уряду. Перехід країн до демократичної системи правління, коли громадянам гарантують участь у державному управлінні через вибори та участь у політичних партіях, створює політичну конкуренцію в суспільстві. За наявності багатьох конкуруючих інтересів перемога жодної політичної сили на виборах не гарантує належної підтримки в суспільстві. У реальних продуктах механізмів консультацій зацікавлені і представники органів влади (передусім політики), і громадянського суспільства, оскільки консультації дають змогу владі краще розуміти потреби й інтереси різноманітних груп населення та визначити пріоритети урядової політики, що ґрунтується на комплексному аналізі очікувань громадян та інших зацікавлених груп [10, с. 264-265].

З метою залучення громадян до участі в управлінні державними справами, Постановою Кабінету Міністрів України [11] було затверджено Порядок проведення консультацій з громадськістю з питань формування та реалізації державної політики. Консультації з громадськістю проводяться з метою залучення громадян до участі в управлінні державними справами, надання можливості для їх вільного доступу до інформації про діяльність органів виконавчої влади, а також забезпечення гласності, відкритості та прозорості діяльності зазначених органів.

Щодо парламенту, то, як показує передовий досвід розвинутих демократичних країн, для функціонування сильних парламентів з якісним прийняттям політичних рішень існує необхідність у залученні громадян до політичного та законотворчого процесу. Аналіз ролі парламенту у майбутньому показує, що одним із провідних факторів його ефективності має стати поява нової концепції представництва, яка має полягати у діяльності на користь тих, кого він представляє, шляхом постійного зв’язку з останніми. Таку повну інтегрованість громадян із парламентарями, яка передбачає постійний дискурс, дуже важко було уявити у добу до поширення Інтернет-технологій. Раціональний дискус пов’язує демократію з громадською участю та забезпечує зв’язок між позицією громадськості та процесом прийняття рішень на національному рівні.

Необхідно зазначити, що протягом останніх років у роботі парламентарів відбулися суттєві зміни формату їхньої роботи та їхньої ролі. Сучасні комунікаційні технології дозволяють громадянам отримати доступ безпосередньо до суб’єктів прийняття рішень. Тому ефективна каналізація інформації навколо парламенту, а також використання нових технічних можливостей наразі є вимогою нинішнього часу. Нині чітко проглядається тенденція до більш тісної комунікації та безпосередньої взаємодії парламентарів з представниками громадськості. Вони набули особливої актуальності у зв’язку з підвищенням уваги до представницької ролі парламенту. Народні обранці дедалі частіше обирають особисті поїздки до виборчих округів з метою підтримки безпосереднього зв’язку з громадськістю.

Можливості комунікувати з парламентарями не лише у виборчий період, а й постійно підтримувати зв’язок з ними он-лайн, спонукає громадян формувати власні позиції та робити оцінки на основі інформації, отриманої з медіа та інших джерел. Це перетворює їх на активних акторів вироблення політики та змушує шукати нові канали впливу на законотворчий процес. Тому майбутнє парламенту буде визначено з урахуванням нових форм неконтрольованої та неієрархічної взаємодії та комунікації. Враховуючи тенденції до інформатизації політичного процесу, основними тенденціями розвитку парламентської комунікації у майбутньому мають стати:

– масштабне оцифровування інформації від самого початку її продукування з активним використанням он-лайн сервісів і оперативним друком документів (у разі необхідності);

– висока інформаційна мобільність через ефективні мережі, а також зростання кількості персональних зустрічей парламентарів з виборцями;

– взаємна інтеграція тих, хто продукує інформацію, та тих, хто її споживає (парламентарів і громадян);

– технічна підтримка буде гнучкою, забезпечуватиметься через швидку адаптацію новітніх технологій до потреб користувачів інформації.

В цілому, роль технологічного потенціалу, спрямованого на максимальне поширення парламентської інформації, має оцінюватися з урахуванням того, що стимулювання інформаційної відкритості парламентів може сприяти змінам, однак не обумовлювати їх. Парламентарі більше схильні оприлюднювати (транслювати) результати власної роботи, аніж безпосередньо контактувати з мільйонним населенням. Водночас он-лайн комунікація не може повністю покрити всі аспекти принципу прозорості та доступності роботи законодавчого органу. У цьому контексті цікавим є досвід створення парламентських кафе в Уганді. “Парламентські кафе” — це новий спосіб підвищення суспільного інтересу до новітніх наукових розробок, який передбачає створення форуму для обговорення актуальних для парламентарів і громадськості питань. Такий форум передбачає дискусії парламентарів і звичайних

громадян з експертами по конкретних питаннях у комфортному для вільної розмови громадському місці (зазвичай, поза аудиторіями та лабораторіями). Такий обмін інформацією передбачає визначення взаємно цікавих моментів для розмови, що сприяє освіті громадян і забезпечує відповідальність експертів і науковців перед суспільством [12, с. 6].

Використання інформаційно-комунікаційних технологій з метою підвищення політичної та операційної ефективності парламентів стало популярним протягом останніх років. Комп’ютери та інші способи дистанційної комунікації у парламентах багатьох країн світу використовувалися десятиліттями, однак, здебільшого, для виконання адміністративних або дуже конкретних завдань (обслуговування персоналу, листування тощо). Зростання масштабів використання комп’ютерів та Інтернету у світі обумовив більшу увагу до можливостей інформаційно-комунікаційних технологій у сфері законотворення. Дедалі більше членів парламенту мають навички використання відповідних ресурсів, що призводить до усвідомлення дивідендів від такого використання (наприклад, у контексті виборів, вирішення питань місцевого значення, визначення національних пріоритетів політичного розвитку тощо). Запровадження використання інформаційно-комунікаційних технологій при необхідному для цього стратегічному плануванні було визнано одним із ключових пріоритетів багатьох парламентів, оскільки могло б підвищити ефективність представництва, а також реалізації парламентом законодавчої функцій.

У контексті законотворення варто пам’ятати, що одним із основних завдань парламенту є розгляд у парламенті пропозицій, які у перспективі можуть стати національними законами. Відповідно способи використання нових технологій на етапі розробки законодавчих пропозицій можуть варіюватися. Наприклад, наявність зведеної електронної бази даних міжнародних стандартів по конкретних питаннях може суттєво допомогти відповідальним за проектування законів у самому парламенті; до того ж, це допоможе подальшому поширенню розробленої документації з метою її друку, оприлюднення в Інтернеті, електронної розсилки тощо. Якщо ж законопроект розробляють поза парламентом, електронні механізми врахування всіх ідей і позицій спрощують процес уніфікації, а також їх поширення серед парламентарів. Базована на інформаційно-комунікаційних технологіях система електронного документообігу підвищує швидкість, точність і гнучкість обміну інформацією між комітетами та депутатами, а також допомагає збільшити час на безпосереднє вивчення пропозицій. Крім того, електронний збір інформації дозволяє отримати максимально повну інформацію про історію конкретної проблеми та оцінки виборців щодо того чи іншого варіанту її вирішення. Ще один позитивний момент – рівність доступу всіх парламентарів до потрібної інформації, що сприяє підвищенню якості парламентських дебатів у комітетах і в сесійній залі. Систематизація інформації про розгляд і проходження законопроектів дозволяє вести повний постійно доступний громадянам електронний архів законодавчого процесу, що спонукає динамічно оцінювати ефективність законодавчого органу [12, с. 7].

Український парламент зробив ще один крок назустріч суспільству, ввівши в дію портал громадського обговорення законопроектів, розроблений за підтримки Програми USAID РАДА та за ініціативи Управління комп’ютерних систем Апарату ВРУ у відповідь на рекомендації Європейського Парламенту щодо внутрішнього реформування Верховної Ради з метою поліпшення її інституційної спроможності. Зазначене надає змогу громадянам заздалегідь ознайомитися з законопроектами, що мають бути внесені на обговорення парламенту, перебувають на розгляді профільних

комітетів, та взяти участь у їх обговоренні. Крім того, зазначене надає можливість поліпшити прозорість діяльності та довіру до комітетів, а це є частиною комплексної програми відкритості комітетів.

У співпраці місцевої влади та громадськості можуть бути різнобічні інструменти. Одним із таких дієвих і основних, на нашу думку, механізмів є місцевий референдум, який є відповідним способом прийняття громадянами рішень з суспільно важливих питань місцевого значення та підзаконних нормативно-правових актів шляхом голосування. Саме через референдум здійснюється народне волевиявлення. На місцевому рівні вони мають бути прерогативою територіальних громад, які мають забезпечувати їх проведення і практичне впровадження їхніх результатів. За своїм змістом місцеві референдуми є формою безпосередньої, прямої, локальної (місцевої) демократії, що передбачає здійснення місцевої публічної влади безпосередньо територіальними громадами в межах відповідних адміністративно-територіальних одиниць. Місцевий референдум є основним засобом локальної нормотворчості територіальної громади, який дозволяє їй брати пряму участь в управлінні місцевими справами. Однак, на сьогоднішній день Верховна рада України, прийнявши у 2012 році Закон України “Про всеукраїнський референдум” і скасувавши Закон України “Про всеукраїнський та місцеві референдуми”, до цього часу не прийняла новий закон, який би враховував законодавство про вибори та об’єктивні реалії місцевого розвитку, а також дозволив би зробити місцевий референдум дієвим механізмом впливу громадян на прийняття рішень. У ньому мають бути враховані такі недоліки попереднього закону, як фактичне унеможливлення проведення референдумів без згоди місцевої влади. Це особливо актуально в нинішніх трансформаційних умовах суспільного життя в Україні. Однак, незважаючи на наявні ускладнення, безпосереднє волевиявлення громадян має ключове значення для ефективного вироблення політики. Тому за новим законом місцевий референдум повинен стати пріоритетною формою волевиявлення територіальної громади при вирішенні локальних проблем. Таким чином створення належних умов для участі членів громад у місцевому управлінні шляхом місцевих референдумів потребує напрацювання сучасного законодавства.

Іншим механізмом є громадська експертиза діяльності органів виконавчої влади, під якою розуміється оцінка діяльності органів виконавчої влади, а також ефективності прийняття та виконання ними рішень з метою підготовки пропозицій щодо розв’язання суспільно значущих проблем. З цією метою та метою створення належних умов для участі громадськості у формуванні державної політики Кабінет Міністрів України прийняв Постанову [13], яка надала організаціям громадянського суспільства можливості бути долученими до розробки та моніторингу державної політики, зокрема – на місцях. З огляду на зазначене громадяни отримують право провести аналіз та дати оцінку роботи органів влади, ефективності прийняття та виконання органами рішень, на основі проведеного аналізу сформулювати пропозиції та визначити необхідні заходи щодо розв’язання проблем у певній сфері державної політики. Органи державної влади повинні сприяти інститутам громадянського суспільства у проведенні відповідного аналізу, надавати необхідну інформацію для проведення експертизи та врахувати підготовлені пропозиції під час вирішення питань поточної діяльності.

Проте згадана Постанова не поширюється на органи місцевого самоврядування, в тому числі сільські, селищні, міські ради, їх виконавчі органи, а є обов’язковою до виконання тільки центральними та місцевими органами виконавчої влади, зокрема

міністерствами та їх територіальними органами, іншими центральними органами виконавчої влади, обласними, районними державними адміністраціями тощо. Для органів місцевого самоврядування Постанова має рекомендаційний характер і може використовуватися ними у питанні проведення громадських експертиз.

Відповідно до проведеного Українським незалежним центром політичних досліджень аналізу, деякі обласні центри України у питанні проведення громадських експертиз діяльності органів місцевого самоврядування (міської ради, міського голови, виконавчого комітету, виконавчих органів міської ради) керуються згаданою Постановою. Зокрема передбаченим Постановою порядком проведення громадських експертиз керуються міста Дніпропетровськ, Житомир, Київ та Кіровоград [14].

Крім проведення експертизи виконавчих органів міських рад, частина міст у своїх статутах територіальних громад серед механізмів участі членів територіальної громади у здійсненні місцевого самоврядування передбачають також участь жителів міста у проведенні громадських експертиз проектів рішень органів місцевого самоврядування. Проте статути міст не визначають порядку проведення відповідних громадських експертиз членами територіальних громад. Крім цього, статути надають право членам громади проводити громадську експертизу виключно щодо проектів рішень міської ради, тобто до моменту їх ухвалення на пленарному засіданні сесії ради. Тому є доцільним надання громадам права проведення громадської експертизи діяльності міської ради та її виконавчих органів, оскільки громадська експертиза передбачає аналіз ефективності імплементації рішень та діяльності органу влади, і за результатами проведеного аналізу надання рекомендацій щодо покращення практик в певній сфері публічної політики.

В цілому законодавство у даній царині має наступні недоліки, які, на думку дослідників [14], доцільно врахувати при удосконаленні його положень:

– законодавство не передбачає обов’язковості врахування результатів громадської експертизи безпосередньо при прийнятті владних рішень. Тобто навіть якщо пропозиції будуть розглянуті на засіданнях органу виконавчої влади, немає гарантії, що вони вплинуть на конкретне вирішення того чи іншого питання;

– у контексті діяльності органів місцевого самоврядування, законодавство про сприяння проведенню громадської експертизи має рекомендаційний характер. Тобто залучення експертного потенціалу громадськості для цієї ланки місцевого управління залежить від політичної волі конкретних посадовців;

– запит на проведення громадської експертизи може бути надісланий лише письмово – тобто використання електронних каналів комунікації є обмеженим. Це не відповідає новітнім тенденціям поширення електронного урядування в Україні та світі;

– законодавство не встановлює фахових вимог до інститутів громадянського суспільства, які ініціюють експертизу, а також їх експертів. Фактично будь-яка легалізована неурядова організація може направити до органу виконавчої влади запит на проведення громадської експертизи. Якщо експертний потенціал інституту громадянського суспільства, що направляє запит, є неналежним, він може залучити зовнішніх експертів, однак прямий обов’язок робити це законодавчо не передбачений. Неспроможність того чи іншого інституту громадянського суспільства забезпечити належну експертизу може дискредитувати важливість цього інструменту співпраці в очах як місцевих органів влади, так і громадськості;

– як правило, проведення громадської експертизи фінансується інститутом громадянського суспільства з власних коштів. Можливість залучення ресурсів з боку зацікавлених осіб є обмеженою, оскільки законодавство відповідних приписів не

містить. Бажання та можливість органу виконавчої влади виділити певні кошти на громадську експертизу залежить від об’єкту, часу та місця її проведення;

– законодавство не передбачає механізмів запобігання конфлікту інтересів під час проведення громадської експертизи. Можливою є ситуація, коли залучені експерти мають професійні або фінансові зобов’язання перед об’єктом експертизи, родинні зв’язки з представниками органів влади тощо. За таких умов, незалежність громадської участі опиняється під загрозою.

Важливим є встановлення зворотного зв’язку з громадянами і в роботі місцевих рад. Для залучення громадян у процес прийняття рішень важливо не лише інформувати громадськість про заплановані консультації, але й розповсюджувати інформацію про результати цих консультацій та забезпечувати зворотній зв’язок не лише з учасниками процесу, а й з ширшою громадою. Потрібно не забувати забезпечувати отримання всіма групами та особами, які були запрошені на захід, протоколу цього заходу та інформації про дії, які будуть вжиті в результаті цього заходу, навіть якщо вони (запрошені) не змогли взяти в ньому участь. Для інформування про подальші дії мають використовуватися засоби масової інформації, включаючи соціальні мережі, веб-сайти, дошки оголошень тощо.

Водночас зазначимо, що закріплений Постановою [11] порядок проведення консультацій є обов’язковим до виконання тільки органами виконавчої влади, а для органів місцевого самоврядування має рекомендаційний характер. З огляду на зазначене у більшості обласних центрів України відсутнє будь-яке правове регулювання питання проведення консультацій з громадськістю та залучення громадян до ухвалення рішень. Відповідно місцевим радам потрібно розробляти власні нормативно-правові акти, що регулюватимуть порядок проведення консультацій з членами територіальної громади щодо питань місцевого значення.

Ще одним механізмом зв’язку з громадськістю є взаємодія з органами самоорганізації населення. Статути територіальних громад обласних центрів України розглядають органи самоорганізації населення як невід’ємну складову системи органів місцевого самоврядування. Комітети заповнюють прогалини у системі представницьких органів самоврядування, адже створюються найближче до життя територіальної громади – на рівні будинку, вулиці, кварталу, мікрорайону, району, чи на рівні невеликого села, селища. Відповідні органи самоорганізації сприяють налагодженню діалогу між представницькими органами влади та безпосередньо громадянами.

Основним нормативно-правовим актом, що регулює порядок створення та діяльності органів самоорганізації населення є Закон України “Про органи самоорганізації населення” [15]. Проте чинний закон містить ряд недоліків, що гальмує розвиток місцевої демократії та перешкоджає самоорганізації членів територіальних громад:

– ускладнена процедура створення органів самоорганізації населення (необхідність проведення декількох загальних зборів (конференцій) громадян за місцем проживання, що включає декілька кроків: ініціювання, подання заяви про створення, отримання дозволу на створення, проведення загальних зборів, на яких створюється орган самоорганізації населення тощо);

– невизначеність правового статусу органів самоорганізації населення, меж їх діяльності, а також розділення повноважень між органами самоорганізації населення різного рівня, що діють на одній території (якщо, наприклад, на певній території діють комітет мікрорайону і будинковий комітет, то за умови рівного правового статусу між ними неодмінно виникатимуть колізії щодо розподілу повноважень та фінансування для належного виконання повноважень);

– відсутність переліку делегованих повноважень органів самоорганізації населення та відсутність чітко визначеного механізму делегування повноважень органами місцевого самоврядування;

– не врегульовано питання гласності роботи і підзвітності органу самоорганізації населення, зокрема в частині розпорядження коштами та майном, господарської діяльності тощо.

За такого законодавства правовий вакуум діяльності органів самоорганізації населення, співпраці з органами місцевого самоврядування можна заповнити через ухвалення відповідних нормативно-правових актів на місцевому рівні, адже відповідно до ст. 4 Закону України “Про органи самоорганізації населення”, комітети діють на підставі рішень відповідних органів місцевого самоврядування, рішень місцевого референдуму, статутів територіальних громад, розпоряджень сільського, селищного, міського голови.

Існує думка, що згаданий Закон не відповідає ні загальнодемократичному принципу правової держави, що “органи влади, їхні посадові та службові особи діють в межах, в спосіб та у порядку, визначеному законом, а громадянам дозволено робити все, що не заборонено законом”, ні вимогам сьогодення.

Як показують реалії життя в Україні, надання місцевими радами дозволу громадянам щодо самоорганізації для забезпечення та відстоювання своїх законних прав та інтересів, які часто ідуть в розріз із ухваленими рішеннями місцевих рад, чи у випадку їхньої бездіяльності щодо існуючих порушень прав громадян – є анахронізмом минулого і потребує правової корекції. Крім того, життя породило нові форми органів самоорганізації громадян (комітети під’їзду або секції; комітети, які поєднали громадян різних будинків і вулиць для вирішення конкретної проблеми – припинення незаконного будівництва, збереження екології в конкретному місці тощо). З огляду на зазначене, є очевидною зміна дозвільного характеру утворення органів самоорганізації на довідковий, що потребує внесення відповідних змін до Закону.

Існують і інші механізми зворотного зв’язку з громадськістю, як то:

– Громадська рада, як постійно діючий колегіальний виборний консультативно-дорадчий орган, утворений для забезпечення участі громадян в управлінні державними справами, здійснення громадського контролю за діяльністю органів влади, врахування позицій громадськості при формуванні та реалізації державної політики. Незважаючи на те, що законодавче зобов’язання для органів виконавчої влади та рекомендація для органів місцевого самоврядування створити громадські ради стало важливим кроком на шляху до посилення участі громадськості у процесі прийняття рішень на місцях, громадські ради наразі ще не повністю стали інструментом дієвого впливу.

Перший досвід їх формування продемонстрував, що, з одного боку, органи влади ще не навчилися максимально ефективно співпрацювати з громадськістю, а з іншого – самі інститути громадянського суспільства виявилися не готовими до належної самоорганізації та кооперації.

– Загальні збори громадян як зібрання усіх чи частини мешканців села (сіл), селища, міста для розв’язання питань місцевого значення; вони є формою безпосередньої участі громадян у розв’язанні питань місцевого значення, і регулюються Законом України “Про місцеве самоврядування в Україні”, Постановою Верховної Ради “Про затвердження Положення про загальні збори громадян за місцем проживання в Україні” та статутами територіальної громади.

Законодавець не наділив загальні збори правом приймати місцеві нормативні акти, але потенційно це може стати найбільш сильною за рівнем впливу на місцеву

владу формою безпосередньої демократії. Основною перевагою зборів як інституту безпосередньої демократії і як форми місцевого самоврядування є органічне поєднання в них колективної соціальної дії: обговорення тієї чи іншої проблеми, відображення колективної думки, прийняття колективного рішення за участі членів територіальної громади.

Висновки.

На підставі проведеного дослідження можна зробити висновок про те, що в сучасних умовах, в умовах реформування влади в Україні, комунікація влади і суспільства є важливим інструментом намічених змін, в яких можна виділити соціальні мережі та інші засоби Інтернет-комунікації. Вони є незамінними для організації масових заходів, для залучення населення в роботу органів влади усіх рівнів.

Соціальні мережі – це, насамперед, робота з людьми, де використовуються методи і підходи, які різняться від тих, що використовуються в традиційних ЗМІ. Це стосується способів подання інформації та стилю спілкування. Сьогодні Інтернет надає широкі можливості використання різного контенту, невимушений стиль спілкування – все це дозволить залучити до взаємодії із органами влади більшої кількості людей, підвищити рівень прозорості такої взаємодії і рівень довіри до органів влади.

За наявності усіх позитивних і негативних моментів здійснення діалогу влади і суспільства за допомогою Інтернет-сайтів, зазначимо, що здійснення діалогу вигідно як для влади, так і для суспільства.

Використана література

1. Угода про коаліцію депутатських фракцій “Європейська Україна” від 27 листопада 2014 р. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/n0001001-15

2. Про ратифікацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Закон України від 16.09.14 р. // Відомості Верховної Ради України (ВВР). – 2014. – № 40. – Ст. 2021.

3. Про Стратегію сталого розвитку “Україна – 2020”: Указ Президента України від 12.01.15 р. № 5/2015 // Офіційний вісник України. – 2015 р. – № 4. – Ст. 67.

4. Меморандум України з МВФ**,** який визначає генеральну економічну лінію влади України в 2014 – 2016 роках. – Режим доступу : http://zn.ua/ ECONOMICS/ opublikovan-polnyy-tekst-memoranduma-ukrainy-i-mvf-144316_.html

5. Володимир Гройсман назвав основні завдання щодо реформи децентралізації на 2016 рік. – Режим доступу : http://rada.gov.ua/news/Top-novyna/122889.html

6. П. Шампань. Делать мнение : новая политическая игра ; [пер. с фр. под ред. Осиповой Н.Г.]. – М. : Socio-Logos, 1997. – 317 с.

7. Кількість користувачів Інтернетом в Україні зростає з рекордною швидкістю. – Режим доступу : http://energolife.info/ua/2016/News/406

8. Киселева А. М., Шпак Е. А. Социальные сети в процессе коммуникации между властью и обществом. – Режим доступу : http://vestnik.uapa.ru/ru/issue/ 2015/06/7

9. Афонін Е.А. Громадська участь у творенні та здійсненні державної політики / Е.А. Афонін, Л.В. Гонюкова, Р.В. Войтович. – К. : Центр сприяння інституц. розвитку держ. служби, 2006. - 160 с.

10. Взаємодія органів державної влади та громадянського суспільства : навч. посіб. / [авт. кол. : Ю.П. Сурмін, А.М. Михненко, Т.П. Крушельницька та ін.] ; за наук. ред. д-ра соц. наук, проф. Ю.П. Сурміна, д-ра іст. наук, проф. А.М. Михненка. – К. : НАДУ, 2011. – 388 с.

11. Про забезпечення участі громадськості у формуванні та реалізації державної політики : Постанова Кабінету Міністрів України від 03.11.10 р. № 996 // Офіційний вісник України. – 2010р. – № 84. – Ст.2945.

12. Чебаненко О. Інформаційний супровід роботи сучасних парламентарів : Часопис ПАРЛАМЕНТ / О. Чебаненко. – К. : Вістка. – № 3/2010.

13. Про затвердження Порядку сприяння проведення громадської експертизи діяльності органів виконавчої влади : Постанова Кабінету Міністрів України від 05.11.08 р. № 976 // Офіційний вісник України. – 2008. – № 86. – Ст. 2889.

14. Інші форми участі членів територіальної громади у місцевому самоврядуванні. – Режим доступу : http://civil-rada.in.ua/?p=2075

15. Про органи самоорганізації населення : Закон України від 11.07.01 р. // Відомості Верховної Ради України (ВВР). – 2001. – № 48. – Ст. 254.

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

УДК 340.11

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

ПРАВОВІ ПРОБЛЕМИ “ЕЛЕКТРОННОЇ ДЕМОКРАТІЇ”

Анотація. *В статті досліджується перспективна форма демократії, яка базується на використанні інформаційних комп’ютерних технологій, обґрунтовуються дефініції базових термінів “інформаційне суспільство”, “демократія”, “електронна демократія”, аналізуються основні правові проблеми розвитку електронної демократії.*

Ключові слова: *демократія, електронна демократія, інформаційне право, ідентифікація.*

Аннотация*. В статье исследуется перспективная форма демократии, основанная на использовании информационных компьютерных технологий, обосновываются дефиниции базовых терминов “информационное общество”, “демократия”, “электронная демократия”, анализируются основные правовые проблемы развития электронной демократии.*

Ключевые слова*: демократия, электронная демократия, информационное право, идентификация.*

Summary. *The article explores a promising form of democracy based on the use of information computer technologies, substantiates the definitions of the basic terms “information society”, “democracy”, “electronic democracy”, analyzes the main legal problems of the development of e-democracy.*

Keywords: *democracy, electronic democracy, information law, identification.*

Постановка проблеми. В Україні, яка є членом Ради Європи, вважають, що розвиток демократичних процесів на засадах застосування загальновизнаної системи демократичних цінностей, зокрема на засадах безумовної участі громадян і громадянського суспільства у процесах формування та реалізації державної політики, відіграє ключову роль у забезпечені економічного та соціального прогресу в державі.

Сучасний міжнародний досвід свідчить, що демократія являє собою найбільш ефективний вид державного устрою, який може приймати різні форми в різних країнах в залежності від політичних і конституційних традицій та який виступає гарантією ефективного проведення реформування держави та суспільства, що є вкрай актуальним як в цілому для України, так і для кожної окремої людини.

Багато країн світу докладають значних зусиль для вдосконалення системи демократії, зокрема і завдяки використанню можливостей інформаційних комп’ютерних технологій (далі – ІКТ). Саме використання ІКТ при здійсненні демократичних процесів призвело до появи такого, хоча і неоднозначного та суперечливого за етимологією, але широковживаного інтернаціонального поняття як “електронна демократія” (далі – е-демократія).

В Україні низку національних, регіональних та галузевих програм спрямовано на широке впровадження ІКТ у всі сфери життєдіяльності суспільства. Тому наша країна має хороший потенціал щодо поширення використання інструментів е-демократії, свідченням чого є те, що в рейтингу ООН у 2016 році Україна покращила свою позицію щодо індексу електронної участі (е-участі) на 45 позицій. Але є низка проблем, зокрема і правових, які створюють певні бар’єри на шляху розвитку е-демократії в Україні.

Проблеми розвитку демократії та “електронної демократії” досліджували М.С. Вершинін, Л.С. Винарик, Н.В. Грицяк, М.В. Дубняк, О.В. Петришин, О.В. Скрипнюк, В.М. Фурашев, В. Швець, Вочевидь, серед багатьох цих проблем особливе місце займають правові, тому вивченню деяких загальних та окремих правових проблем е-демократії були присвячені роботи Я.В. Антонова, К. А. Бабенко, С.А. Дятлова, Ж.О. Панченко. Нормативно-правовою базою розвитку е-демократії є низка національних та міжнародних актів [13, с. 31].

Наявність різноманітності підходів та різновекторності рекомендацій щодо вдосконалення правового регулювання потребують певного теоретико-методологічного узагальнення щодо визначення поняття “електронна демократія”, напрямків вирішення правових проблем її розвитку, що з огляду на важливість застосування інструментів е-демократії для сучасного етапу розвитку України має актуальне значення.

Метою статті є визначення дефініцій базових термінів та основних правових проблем розвитку “електронної демократії”.

Виклад основного матеріалу. Найчастіше поняття “електронна демократія” розглядається з позиції двох парадигм. За першою, “електронна демократія” – це самостійна форма демократії за умови використання інформаційно-комунікаційних технологій [5]. При цьому поширеною є думка про використання ІКТ лише як засобу комунікації. Так, наприклад, М. Вершинін вважає, що “електронна демократія” – це будь-яка демократична політична система, в якій комп’ютери і комп’ютерні мережі використовуються для виконання найважливіших функцій демократичного процесу, таких як поширення інформації та комунікація [5]. В роботі С.А. Дятлова прямо припускається, що використання ІКТ в демократичному процесі призводить до його трансформації з традиційного в “електронну демократію” або “інформаційно-мережеву демократію” [10].

За другою парадигмою – “електронна демократія” розглядається в якості підтримки та розширення демократії за допомогою ІКТ [7, 17, 31]. Саме така концептуальна позиція вбачається нам такою, що найбільше відповідає змісту використання ІКТ у будь яких процесах, зокрема і демократичних.

Термін “електронна демократія” є складним, який складається з двох: “електронний” та “демократія”.

Сучасна правова наука оперує декількома моделями демократії, а визначаючи дефініцію власне самого поняття “демократія” різні дослідники можуть мати подекуди доволі відмінні уявлення про неї та про те, як вона функціонує [22].

Наприклад, Н.М. Крестовська вважає, що виходячи із позицій сучасної юриспруденції, “демократія” – це такий тип держави, за якого всі без винятку громадяни беруть участь у формуванні і функціонуванні апарату органів державної влади і місцевого самоврядування, і здійснюють контроль над його діяльністю [13, с. 31]. В цьому контексті визначають наступні принципи демократії: 1) народного суверенітету; 2) політичної свободи і рівності громадян; 3) плюралізму у всіх сферах суспільного життя; 4) свободи слова, гласності та відкритості діяльності всіх суб’єктів політики; 5) виборність органів державної влади і органів місцевого самоврядування; 6) поділу влади; 7) підзвітності і підконтрольності; 8) ухвалення рішень більшістю з урахуванням прав меншості; 9) підпорядкування меншості більшості при ухваленні рішень [21].

Український вчений В.Д. Щвець відносно демократії дійшов наступних висновків: політичний режим є демократичним тільки в разі, якщо він представляє інтереси широких верств населення; демократія виходить з цінності кожної людини, тому прагне до створення цивілізованих умов життя для всіх громадян незалежно від

багатства і таланту; демократія повинна пов’язуватись не тільки з демократією в політичній сфері, а й в економічній, соціальній, культурній та інших галузях життєдіяльності суспільства [28].

За думкою К.А. Бабенко відповідно до Конституції Україна визначається як демократична держава, що передбачає обов’язкове закріплення на рівні найвищого закону країни ряду принципів та інститутів, які є невід’ємними властивостями організації демократичної влади та функціонування демократичної системи врядування [2]. Навіть не надючи визначення терміну “демократія”, К.А. Бабенко наполегливо акцентує увагу на демократичному характері влади та врядування, які, як відомо, є інституціями соціуму, що насамперед призначені для прийняття та втілення в життя рішень з різноманітних питань.

Для подальшого дослідження є вкрай важливою думка О.В. Петришина про те, що громадяни у демократичній державі погоджуються не лише на прийняття якогось певного рішення, прийнятого шляхом голосування більшості, а й на відповідну систему демократичного ухвалення рішень, унормовану конституцією і законом [18].

На нашу думку, при цьому звертається увага не лише на голосування як фінальний етап демократичного процесу прийняття рішень, але і на не менш важливу частину цього процесу, яка іноді є вирішальною – весь підготовчий процес формування, прийняття та виконання рішень. При цьому регламентація процесу формування, прийняття та виконання рішень, на його думку повинна бути здійснена на нормативно-правовому рівні.

ООН в своєму Підсумковому документі Всесвітнього саміту 2005 р. визначає, що “демократія – це універсальна цінність, заснована на вільному волевиявленні народу, який визначає свої політичні, економічні, соціальні та культурні системи, і на його активній участі у вирішенні питань, що стосуються всіх аспектів його життя” [32]. Таким чином, світове співтовариство підкреслює суверенне право народу кожної держави брати участь у процесі прийняття рішень з будь-яких питань, що стосуються його життя.

Отже, характерною рисою демократії є демократичний спосіб прийняття рішень за умови участі всього населення в процесі прийняття рішень, що, в переважній більшості випадків, передбачає на нормативно-правовому рівні, як визначення способу та форми власне прийняття самого рішення, так і визначення системи процедур (алгоритмів) щодо всіх етапів процесу прийняття рішення. На наш погляд, найбільш повно та змістовно перелік таких етапів процесу прийняття рішень було запропоновано М.В. Дубняк, до яких вона відносить: визначення проблемного питання (пропозиції); внесення пропозиції на розгляд; збір альтернативних проектів вирішення проблеми; аналіз альтернативних проектів вирішення проблеми та їх рейтингування; розробку проекту рішення; прийняття рішення; оприлюднення прийнятого рішення; виконання рішення; контроль за виконанням; коригування плану виконання на будь-якому проміжному етапі [9].

Таким чином, в цілому погоджуючись із думкою багатьох вчених-юристів про те, що єдиного загальновизнаного визначення терміну “демократія” не існує, з врахуванням вищевикладеного в інтересах даного дослідження запропонуємо наступне визначення: *демократія* – організація життєдіяльності суспільства (окремої соціальної групи), що базується на методі колективного прийняття рішень, який передбачає рівне право всіх членів суспільства на участь і рівний ступінь впливу на всіх етапах процесу прийняття рішення і його виконання за умови створення рівних можливостей для обміну думками,

доступу до всієї необхідної інформації, участі в оцінці та відборі альтернативних варіантів рішень і в остаточному голосуванні.

Формулювання дефініції терміну “електронна демократія” потребує відповідного попереднього пояснення. В останні десятиріччя одержали широке поширення такі неологізми як е-суспільство, е-економіка, е-медицина і багато інших, які є образними і ємними відображенням повсюдного впливу ІКТ на людську діяльність [14, 23, 24, 25]. Потім з’явилися похідні від цих неологізмів: “електронний уряд”, “електронна митниця”, “електронний лікар”, “електронний бізнес”, “електронна торгівля”, зокрема і “електронна демократія” [8, 14, 23]. Беззаперечно, потужним каталізатором використання зазначених неологізмів є надзвичайне широке розповсюдження ідеї інформаційного суспільства.

У минулому столітті людство дійшло до такої межі в своєму розвитку, коли традиційні методи, способи і засоби збирання, зберігання, обробки та поширення інформації перестали задовольняти його потреби. Це було обумовлено тим, що в багатьох сферах суспільної діяльності при прийнятті рішень необхідно стало враховувати вплив значної кількості факторів на ті чи інші процеси, що потребувало обробки великих масивів інформації, нерідко, в режимі реального часу. Відповіддю на цю проблему стала поява електронно-обчислювальних машин. Надзвичайно високими темпами поширилось впровадження та використання ІКТ. Все це і стало причиною того, що наступну фазу розвитку людського суспільства після постіндустріальної здебільше визначили як інформаційне суспільство.

Саме Е. Тоффлер виділив три стадії у розвитку людства: аграрну, індустріальну і постіндустріальну [25]. Наприкінці минулого століття в світі поширилася думка про те, що людство йде в інформаційне суспільство і XXI століття буде століттям ІКТ. Вивченню проблематики інформаційного суспільства присвячено багато робот, особливе значення серед них мають ті, які приділяють увагу системним наслідкам упровадження інформаційних технологій у різні сфери життя суспільства [6, 11, 14, 15, 23, 24 тощо].

Історично одне з найперших вдалих визначень терміну “інформаційне суспільство” було надано в Європейському Союзі. “Інформаційне суспільство – це суспільство, в якому діяльність людей здійснюється на основі використання послуг, за допомогою інформаційних технологій і технологій зв’язку” [12]. Але це визначення не охоплює діяльність державних органів, громадських інститутів тощо. У відомій Декларації принципів є таке визначення: “інформаційне суспільство – це суспільство, в якому кожен може скористатися можливостями, які можуть надати інформаційно-комунікаційні технології” [8].

Слід зауважити, що чинемала кількість теоретиків вважає, що інформаційне суспільство – це суспільство нового соціального укладу, суспільство, в якому докорінно можуть змінитись соціальні відносини. На хвилі такого сприйняття багато процесів, пов’язаних з використанням ІКТ, надмірно містифікувалося. Часто-густо вони оголошувалися мало не панацеєю для “лікування” всіх недоліків, властивих сучасному стану розвитку соціуму.

Події останніх років принесли цілком закономірне розчарування прихильникам таких поглядів на зміст інформаційного суспільства, підтверджуючи справедливість висновків американського соціолога Ф. Уебстера про те, що “інформаційне суспільство не є суспільством нового типу, воно швидше демонструє результати впливу широкого впровадження інформаційних технологій на соціальні процеси, які практично не міняють свого корінного змісту” [26].

З іншого боку, низка дослідників продовжує наполягати на продуктивності концепції інформаційного суспільства, проте відзначаючи, що відсутність стрункості та строгої наукової обґрунтованості соціальних теорій “інформаційного суспільства” призвела до певної екзальтації в сприйнятті його цінностей [30]. На думку Л. Карвалікса, сьогодні не можна виділити жодне з визначень терміну “інформаційне суспільство”, яке б могло задовольнити всіх і поширювалося б на всі підсистеми соціуму, але цілком можливо дати таке визначення, яке б відповідало інтересам дослідження конкретних підсистем [30].

На наш погляд, невизначеність з дефініцією терміну “інформаційне суспільство” обумовлена значною динамікою проникнення ІКТ в усі сфери життєдіяльності людини, суспільства і держави, що призводить до появи найрізноманітніших нових явищ в соціальній, економічній, культурній, державній, виробничій та інших сферах. Власне такі явища іноді демонструють появу нової соціальної якості в цих сферах. Ця нова якість має різний рівень системності та різний рівень значення для певних сфер життєдіяльності соціуму. Але, саме в силу новизни, найчастіше тільки на них і концентрується увага дослідників, що призводить до гіперболізації досліджуваних явищ.

Саме такі обставини і призвели до поширення термінів “електронний уряд”, “електронна демократія”, “електронний парламент”, “електронна торгівля”, “електронний бізнес”, “електронний суд” і, навіть, “електронна держава”. Тобто термінів, які адекватно не відображають сукупної, системної сутності змісту процесів, що відбуваються.

Не претендуючи на загальний характер такого висновку, зауважимо, що для правових наук використання подібних термінів є причиною появи істотних ускладнень та численних дискусій. Але з огляду на те, що саме в такому вигляді такі терміни вже увійшли до наукового обороту в частині змісту їх дефініцій потрібно висувати підвищенні вимоги щодо їх обґрунтованості.

На нашу думку, до оцінки процесів, пов’язаних з широким впровадженням ІКТ в усі сфери життєдіяльності людини, суспільства і держави, слід підходити з діалектичних позицій. Вивчаючи ту чи іншу сферу, в якій широко використовуються ІКТ, доцільно досліджувати процеси появи і накопичення кількості нових явищ, а також появи нової якості таких явищ. При цьому потрібно відповісти на питання: чи викликала поява нових явищ підвищення якісних показників традиційних суспільних характеристик цієї сфери або ж вона призвела до виникнення якісно нових характеристик? Потім, у свою чергу, треба відповісти на наступне питання: чи не призвело накопичення кількості якісно нових суспільних характеристик до зміни сутності самої сфери, до зміни її якісного і змістовного стану? Тільки після вивчення зазначених аспектів наслідків впровадження інформаційних комп’ютерних технологій стає можливим оцінити зміни окремо в соціальній, економічній, культурній, державній, виробничій та інших сферах, а згодом – і в цілому, в соціумі. Наявність такого детального та системного аналізу може дозволити обґрунтувати висновок про зміну або не зміну соціального укладу.

Одне можна сьогодні стверджувати досить впевнено – використання ІКТ в найрізноманітніших сферах діяльності людини, суспільства і держави суттєво підвищує її ефективність і часто привносить нову якість, що визначає нагальну необхідність враховування цього, як при реалізації суспільних відносин та їх вивченні, так і при прогнозуванні їх розвитку.

Запропонований підхід до аналізу наслідків впровадження ІКТ дозволяє з’ясувати та пояснити існування двох діаметрально протилежних позицій щодо змісту поняття “інформаційне суспільство”, різних підходів до стратегії розвитку та різного

акцентування його цінностей: демократичних, економічних, технократичних, культурологічних, комунікативних тощо.

З урахуванням зазначеного, а також на основі результатів вивчення матеріалів міжнародних документів, праць вчених, у тому числі юристів, на основі дослідження змісту процесів, пов’язаних із широким впровадженням ІКТ в найрізноманітніших сферах, надаємо наступне визначення терміну “інформаційне суспільство” в інтересах юридичної науки. *Інформаційне суспільство* – це суспільство, в якому вся сукупність суспільних відносин з метою підвищення ефективності людської діяльності в різних сферах (політиці, економіці, публічному управлінні, військовій справі, освіті, культурі, розвагах, особистому житті тощо) реалізується на основі максимального використання інформаційних комп’ютерних технологій [33].

Виходячи із цього визначення, стає зрозумілим, що в умовах поширення цінностей інформаційного суспільства всі суспільні відносини, які засновані на використанні інформації, прагнуть реалізовувати за допомогою сучасних ІКТ. Можна навести безліч прикладів із різних сферах людської діяльності, які демонструють значне підвищення ефективності результатів тих чи інших суспільних відносин завдяки застосуванню ІКТ. Таким чином, діалектика суспільного розвитку на сучасному етапі свідчить про те, що подальший прогрес людства однозначно тісно пов’язаний з широким впровадженням ІКТ, або, іншими словами, з побудовою інформаційного суспільства. Повною мірою це відноситься й до суспільних відносин, пов’язаних з демократичними процесами, тобто до тих процесів, що отримали назву електронна демократія.

В розпорядженні Уряду “Про схвалення Стратегії розвитку інформаційного суспільства” надано наступне визначення: “електронна демократія – форма суспільних відносин, за якої громадяни та організації залучаються до державотворення та державного управління, а також до місцевого самоуправління шляхом широкого застосування інформаційно-комунікаційних технологій”.

Вважається, що саме “електронна демократія” за умови застосування всього спектру сучасних інструментів, що використовують ІКТ, створює підґрунтя для ефективного втілення в життя великої кількості різноманітних традиційних видів безпосередньої демократії, зокрема таких як вибори, референдуми, виявлення громадської думки, плебісцити, народні обговорення, народні ініціативи, петиції (колективні письмові звернення), збори тощо [19]. Крім того, ІКТ дозволяють використовувати такі новітні інструменти електронної демократії як електронні консультації, Інтернет-конференції, відеоконференції, електронні засоби зворотного зв’язку, електронна пошта, дискусійні форуми на веб-сайтах, електронні опитування громадської думки тощо.

Зазначені інструменти електронної демократії, як традиційні, так і нові за певних умов допомагають залучити до процесу прийняття рішень максимальну кількість населення, якого ці рішення можуть безпосередньо стосуватись.

Таким чином, гармонійне поєднання різноманітних інструментів електронної демократії як певних форм безпосередньої демократії та форм традиційної представницької демократії надає змогу мінімізувати певні недоліки останньої.

Враховуючи надані раніше визначення термінів “демократія” та “інформаційне суспільство”, запропонуємо наступну дефініцію: *електронна демократія* – це демократія, для якої значно підвищується ефективність демократичних інститутів, демократичних процесів та поширення демократичних цінностей за умови застосування різноманітних інструментів, що базуються на максимальному використанні інформаційних комп’ютерних технологій.

Зазначеним визначенням стверджується, що зміст (сутність) демократії в умовах електронної демократії визначається тією моделлю демократії традиційної форми (без використання ІКТ), яка реалізована на даний час у суспільстві. А введення сучасних ІКТ в суспільні відносини призводить до різкого підвищення якості інформаційної взаємодії суб’єктів демократичних процесів, що, в свою чергу, обумовлює підвищення їх ефективності в рамках. Таким чином, ефективність електронної демократії детермінується насамперед моделлю демократії, яка реалізована на даний час у суспільстві, та можливостями ІКТ, які застосовуються.

Але треба звернути увагу на одну феноменальну обставину застосування ІКТ, яка створює потенційні умови навіть для зміни моделі демократії. З огляду на те, що ІКТ та Інтернет-технології створюють реальні можливості інформаційного охоплення населення практично без часових, просторових, фінансових та організаційних обмежень, в соціумі створюються технологічні умови для здійснення часткового або повного переходу від представницької демократії до прямої.

Вбачається, що у найближчому майбутньому буде поширюватись модель із змішаною формою демократії з переважним акцентуванням на формах прямої демократії, особливо для обмежених за функціональним спрямуванням суспільних угрупувань (місцеві, районні та регіональні громади, колективи тощо), яка буде базуватись на широкому використанні можливостей ІКТ.

Погоджуючись з багатьма науковцями щодо перспективності електронної демократії, можна констатувати наявність наступних системних бар’єрів щодо її поширення в Україні:

невизначеність публічної політики у сфері електронної демократії, а також перспективних шляхів її реалізації;

недосконаліть правового забезпечення сфери електронної демократії, насамперед, недосконаліть системи нормативно-правового регулювання;

низький рівень залучення суб’єктів громадянського суспільства до процесів вдосконалення публічної політики у сфері електронної демократії, а також до імплементації її окремих інструментів;

недостатній рівень розвитку інформаційної інфраструктури, нерівність проникнення доступу до мережі Інтернет та до інформаційних комп’ютерних технологій як основних умов забезпечення розвитку електронної демократії;

низький рівень обізнаності у суспільстві щодо змісту та особливостей використання різноманітних інструментів електронної демократії, а також методів та допоміжних засобів їх застосування;

недостатність мотиваційних важелів, рівня знань та навичок у державних службовців, посадових осіб місцевого самоврядування, громадян щодо розвитку електронної демократії.

Серед сукупності названих основних проблем, безперечно, вкрай важливою є проблема удосконалення правового регулювання суспільних відносин при реалізації демократичних процесів в умовах використання ІКТ. Тому неможливо в частині електронної демократії не погодитись з думкою К.А. Бабенко про те, що однією з найбільш гострих проблем сьогодення, що пов’язані із постанням України як демократичної держави є, насамперед, забезпечення практичної реалізації тих норм і принципів, які проголошено і юридично закріплено на конституційному рівні [2].

В аналітичній записці “Розвиток електронної демократії в Україні” стверджувалось, що в державі функціонування власне електронних форм демократії практично не внормоване, однак існує чимала нормативно-правова база, що регламентує

розвиток інформаційного суспільства й уможливлює реалізацію певних принципів та інструментів е-демократії [20].

Деякі дослідники демонструють неоднозначне розуміння впливу використання ІКТ на зміст правового регулювання суспільних відносин при реалізації демократичних процесів. Наприклад, Я.В. Антонов, погляди якого є найбільш показовими, вважає, що існує правова невизначеність щодо впливу електронної демократії на конституційні обов’язки посадових осіб або щодо наявності конституційного обов’язку у посадових осіб відносно виконання рішення, яке прийнято за допомогою ІКТ [1].

Такий підхід створює хибну уяву про те, що начебто може існувати різне за сутністю правове регулювання суспільних відносин, пов’язаних з демократичними процесами, в залежності від використання ІКТ. Але доведено, що основний зміст правового регулювання не залежить та не змінюється від використання ІКТ або Інтернет-технологій, які власне впливають лише на якість інформаційної взаємодії суб’єктів суспільних відносин [3]. А в умовах “електронної демократії” можуть з’явитись лише особливості правового регулювання традиційних демократичних процесів и лише в частині суспільних відносин, пов’язаних з інформацією та інформаційними процесами, що є складовими цих процесів. До таких специфічних особливостей правового регулювання при застосуванні ІКТ, наприклад, як вважає А. Церрилло, повинні бути створені умови щодо дотримання правових принципів, цілісності та автентичності документів, конфіденційності даних [29].

Загальновизнано, що суспільні відносини, пов’язані з інформацією, інформаційними процесами, використанням ІКТ регулюються нормами інформаційного права. Тому цілком закономірним є висновок про те, що загальні проблеми напрямів вдосконалення перспективних досліджень як теоретико-методологічних проблем інформаційного права, так і проблем нормативно-правового регулювання, які мають важливе прикладне значення для сфери електронної демократії [4].

Беззаперечно, до фундаментальних прав людини відносяться: свобода слова (створення інформації), свобода доступу до інформації, її використання та розповсюдження (право на інформацію), а також право на її збереження, що є атрибутивним правом будь-якого суб’єкту інформаційних відносин. Зазначене право мало бути реалізованим для всіх суб’єктів суспільних відносин протягом всього часу існування цивілізації, а не лише в суспільстві певної стадії демократичного розвитку. Сукупність зазначених прав означає, що кожен суб’єкт демократичного соціуму має право на отримання в необхідний для нього момент часу неспотвореної та в повному обсязі будь-якої інформації (своєчасної, повної та достовірної інформації).

Інклюзивна участь громадськості в процесі прийняття рішень передбачає повний та безбар’єрний доступ до публічної інформації органів державної влади та місцевого самоврядування, який можна забезпечити інструментами електронної демократії. Задля цього необхідно переглянути правові принципи організації такого доступу, насамперед, передбачивши правові механізми реалізації проактивних методів надання громадськості публічної інформації за допомогою Інтернет-технологій, оприлюднення та постійної актуалізації публічної інформації у вигляді структурованого масиву даних (Big Data, відкриті дані) у форматах, які пристосовані для використання у комп’ютерних системах.

Ефективність функціональної взаємодії в рамках демократичних процесів залежить від якості правового регулювання інформаційної взаємодії на базі ІКТ між суб’єктами соціуму. При цьому важливим є вичерпне визначення прав, обов’язків та відповідальності суб’єктів відповідних правовідносин в процесі інформаційної взаємодії.

В умовах електронної демократії потребують дослідження правові проблеми, що обумовлені використанням Інтернет та пов’язані: а) з невизначеністю місця знаходження суб’єктів (суб’єктів різноманітних опитувань, учасників виборів, учасників подання петицій тощо); б) невизначеністю часу відправлення та отримання інформаційних матеріалів суб’єктами інформаційної взаємодії; в) певним анонімним характером суб’єкта, яка бере участь в інформаційній взаємодії (проблема ідентифікації суб’єкта); г) невизначеністю відносно достовірності отриманої інформації при передачі її засобами ІКТ, при розміщенні її на веб-сайтах тощо.

Висновки.

Основною умовою забезпечення ефективності демократії є всеосяжне поширення в країні демократичних інститутів, демократичних процесів та демократичних цінностей, охоплення ними всіх суспільно значущих процесів і відносин та всіх громадян. В сучасних умовах таке поширення можливо забезпечити лише на засадах широкого застосування інформаційних комп’ютерних технологій у всіх демократичних процесах.

Запропоновані в роботі дефініції термінів “інформаційне суспільство”, “демократія” та “електронна демократія” не обов’язково кращі або точніші за багато інших, але вони найкращим чином підходять для предметної сфери правового регулювання, пов’язаної з електронною демократією, зокрема у сфері публічного управління.

Застосування інструментів електронної демократії як на рівні держави, так і на рівні громад надає потенційні можливості залучення максимально широких верств населення до процесу прийняття рішень з різноманітних питань життєдіяльності суспільства, що в свою чергу створює реальні умови для дієвої реалізації принципу безпосередньої демократії в певних випадках прийняття рішень, а також в багатьох випадках підготовки та виконання рішень, особливо на місцевому рівні.

Забезпечення ефективного застосування інструментів електронної демократії, які фактично представляють собою різноманітні інструменти інформаційної взаємодії, що базуються на використанні ІКТ, потребує вирішення теоретико-методологічних та практичних проблем правового регулювання відповідних інформаційних відносин, що в умовах розвитку демократії в Україні є вкрай актуальним.

Використана література

1. Антонов Я.В. Правовые аспекты электронной демократии и электронного голосования / Управленческое консультирование. – 2014. – № 6. – Режим доступу : http://cyberleninka.ru /article/n/pravovye-aspekty-elektronnoy-demokratii-i-elektronnogo-golosovaniya

2. Бабенко К.А. Конституційне закріплення демократичних основ організації державної влади (теорія і практика реалізації) / К.А. Бабенко // Часопис Київського університету права : Український науково-теоретичний часопис . – 2006. – № 4. – С. 68-74 .

3. Баранов А.А. Интернет : объект правоотношений и предмет регулирования : монография / А.А. Баранов. – К. : Ред. журн. “Право Украины”, 2013. – 144 с.

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

5. Вершинин М.С. Политическая коммуникация в информационном обществе: перспективные направления исследований : сборник научных трудов [“Актуальные проблемы теории коммуникации”]. – СПб. : Изд-во СПбГПУ, 2004. – С. 98-107. – Режим доступу : http://www.russcomm.ru/rca_biblio/v/vershinin02.shtml

6. Винарик Л.С. Вхождение Украины в информационное общество / Л.С. Винарик, А.Н. Щедрин, Н.Ф. Васильева. – Донецк : ИЭП НАН Украины, 2001. – 151 с.

7. Грицяк Н.В. Електронна демократія як механізм політичної взаємодії : навч.-метод. рек. / Н.В. Грицяк, С.Г. Соловйов. – К. : НАДУ, 2013. – 44 с.

8. Декларация принципов. Построение информационного общества – глобальная задача в новом тысячелетии. – (Всемирная встреча на высшем уровне по вопросам информационного общества. Женева, 2003. ; Документ WSIS-03/GENEVA/DOC/4-R. 12 декабря 2003 года). – Режим доступу : http://www.itu.int/wsis/documents/doc_multi.asp?lang=en&id=1161|1160

9. Дубняк М.В. Соціально-правова модель прийняття рішень у місцевому самоврядуванні // Право і суспільство. – №1. – 2017. – С. 149-153.

10. Дятлов С.А. Информационное право в системе отношений электронного правительства и институтов гражданского общества. – (Интернет и современное общество, 2008). – Режим доступу : http://www.ict.edu.ru/vconf/files/10354.pdf

11. Еріксон Т. Тиранія моменту : швидкий і повільний час в інформаційну добу / Т. Еріксон. – Львів : Кальварія, 2004. – 196 с.

12. Європа на шляху до інформаційного суспільства : збірник документів Європейської Комісії 1994 – 1995 рр. ; укл. В.М. Павлович, А.В. Цвігун ; за заг. ред. О.М. Гальченко. – К. : Державний комітет зв’язку та інформатизації України, 2000. – 176 с.

13. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.

14. Кастельс М. Галактика Интернет : размышления об Интернете, бизнесе и обществе / М. Кастельс ; под ред. В. Харитонова . – Екатеринбург : У-Фактория. – 2004. – 328 с.

15. Кастельс М. Информационная эпоха : экономика, общество и ку-льтура / М. Кастельс. – М. : ГУ ВШЭ, 2002. – 608 с.

16. Крестовська Н.М. Теорія держави і права : елементарний курс / Н.М. Крестовська, Л.Г. Матвеева. – [2-е вид.] – Х. : ТОВ “Одіссей”, 2008. – 432 с. – Режим доступу : http://studies.in.ua/krestovska-nm-teorja-derzhavi-prava.html

17. Панченко Ж.О. Правові та соціально-політичні аспекти впровадження електронної демократії в Україні // Актуальні проблеми міжнародних відносин. – 2011. – Вип. 103(1). – С. 94-107. – Режим доступу : http://nbuv.gov.ua/UJRN/apmv_2011_103(1)_15

18. Петришин О.В. Демократичні основи правової, соціальної державності // Вісник Національної академії правових наук України. – 2014. – № 1 (76). – С. 32-41. – Режим доступу : http://dspace.nlu.edu.ua/bitstream/123456789/6466/1/Petryshyn_32.pdf

19. Погорілко В.Ф. Конституційне право України : підручник / В.Ф. Погорілко, В.Л. Федоренко. – [2-е вид., переробл. та доопр.]. – К. : Прав. єдність : Алерта, 2010. – 432 с. – Режим доступу : http://pidruchniki.com/14940511/pravo/formi_bezposerednoyi_demokratiyi_ukr ayini

20. Розвиток електронної демократії в Україні : аналітична записка. – К. : НІСД, 2010. – Режим доступу : http://old.niss.gov.ua/monitor/January2010/01.htm

21. Скакун О.Ф. Теорія держави і права : підручник / О.Ф. Скакун ; [пер. з рос.]. – Харків : Консум, 2001. – 656 с. – Режим доступу : http://pidruchniki.com/70706/pravo/demokratichna_der zhava#14

22. Скрипнюк О.В. Демократія : Україна і світовий вимір (концепції, моделі та суспільна практика) / О.В. Скрипнюк. – К., Логос. – 2006. – 368 с.

23. Стоуньер Т. Информационное богатство : профиль постиндустриальной экономики. Новая технократическая волна на западе / Т. Стоуньер. – М. : Прогресс, 1986. – 450 с.

24. Танскотт Д. Электронно-цифровое общество. Плюсы и минусы сетевого интеллекта / Д. Транскотт. – К. : INT Пресс. – М. : Рефл. Бук, 1999. – 432 с.

25. Тоффлер Э. Третья волна / Э. Тоффлер. – М. : АСТ, 2004. – 781 с.

26. Уэбстер Ф. Теории информационного общества / Ф. Уэбстер. – М. : Аспект Пресс, 2004. – 400 с.

27. Електронне інформаційне суспільство України : погляд у сьогодення і майбутнє / [В.М. Фурашев, Д.В. Ланде, О.М. Григор’єв, О.В. Фурашев]. – К. : “Інжиніринг”, 2005. – 164 с.

28. Швець В. Особливості становлення демократії та впровадження демократичних цінностей в Україні й світі / В. Швець, Ю. Шайхалієва // Віче. – 2010. – № 17. – С. 13-16. – Режим доступу : http://nbuv.gov.ua/UJRN/viche_2010_17_8

29. Cerrillo A. E-Justice: Using Information Communication Technologies in the Court System / A. Cerrillo, H. Fabra. – Hershey ; New York : Information science reference, 2009. – P. 13. – Режим доступу : https://www.safaribooksonline.com/library/view/e-justice-using-information/97815990499 84

30. Karvalics L. How to defend the original, multicriteria theories of Information Society? / L. Karvalics. – (3rd ICTs and Society Meeting; Paper Session – Theorizing the Internet, 2010). – Режим доступу : http://triple-c.at/index.php/tripleC/article/viewFile/214/173

31. Recommendation CM/Rec(2009)1 of the Committee of Ministers to member states on electronic democracy (e-democracy). – (Adopted by the Committee of Ministers on 18 February 2009 at the 1049th meeting of the Ministers’ Deputies). – (Офіційний веб-сайт Ради Європи). – Режим доступу: https://www.coe.int/t/dgap/democracy/Activities/GGIS/CAHDE/2009/RecCM2009_1_and_Accomp_Docs/Recommendation%20CM_Rec_2009_1E_FINAL_PDF.pdf

32. UN General Assembly, 2005 World Summit Outcome : resolution. – (Adopted by the General Assembly, 24 October 2005, A/RES/60/1) – Режим доступу : http://www.refworld.org/docid /44168a910.html

33. Баранов О.А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія / О.А. Баранов. – К. : Едельвейс, 2014. – 497 с.

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

УДК 342.721: 681.3.02

МЕЛЬНИК К.С., *доктор філософії (Ph.D) з юридичних наук*

ОБРОБКА ТА ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В ПРОЦЕСІ ВЕРИФІКАЦІЇ СОЦІАЛЬНИХ ВИПЛАТ ГРОМАДЯН

Анотація. *В статті здійснено аналіз проблемних аспектів обробки та захисту персональних даних в процесі верифікації соціальних виплат громадян, запропоновано шляхи подолання можливих негативних наслідків порушення приватності та інформаційної безпеки людини.*

Ключові слова: *персональні дані, захист персональних даних, обробка персональних даних, соціальні виплати, верифікація соціальних виплат, приватність, інформаційна безпека людини.*

Аннотация. *В статье осуществлен анализ проблемных аспектов обработки и защиты персональных данных в процессе верификации социальных выплат гражданам, предложены пути преодоления возможных негативных последствий нарушения приватности и информационной безопасности человека.*

Ключевые слова: *персональные данные, защита персональных данных, обработка персональных данных, социальные выплаты, верификация социальных выплат, приватность, информационная безопасность человека.*

Summary. *The article presents the analysis of the problematic aspects of the processing and protection of personal data in the process of verification of social payments to citizens, suggests the ways to overcome the possible negative consequences of violations of privacy and information security of person.*

Keywords: *personal data, personal data protection, processing of personal data, social payments, verification of social payments, privacy, information security of person.*

Постановка проблеми. Питання інформаційної безпеки людини та захисту її приватного життя в нашій державі з останніми роками набуває дедалі вагомішого значення. Особливої ваги зазначене питання набуває, коли потенційними порушниками виступають суб’єкти державної влади, тобто держава, яка, навпаки, має охороняти право на недоторканність приватного життя своїх громадян. Варто нагадати, що відповідно до статті 3 Конституції України права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов’язком держави [1].

У грудні 2016 року з засобів масової інформації та офіційної інформації Уповноваженого Верховної Ради України з прав людини стало відомо про безпрецедентне порушення прав на захист персональних даних та приватне життя *внутрішньо переміщених осіб* (далі – ВПО) [2 – 3]. Внутрішньо переміщеною особою є громадянин України, іноземець або особа без громадянства, яка перебуває на території України на законних підставах та має право на постійне проживання в Україні, яку змусили залишити або покинути своє місце проживання у результаті або з метою уникнення негативних наслідків збройного конфлікту, тимчасової окупації, повсюдних проявів насильства, порушень прав людини та надзвичайних ситуацій природного чи техногенного характеру [4].

Так, за інформацією громадських організацій, останнім часом ВПО почали отримувати дзвінки від ТОВ “Дельта М Юкрейн” на номери телефонів, які вони повідомляли *органам соціального захисту при взятті їх на облік*. Співробітники цієї

компанії, посилаючись на ініціативу Міністерства фінансів України привітати їх із новорічними святами, просили уточнити місце перебування таких громадян та іншу конфіденційну інформацію про особу. При цьому, якщо абонент відмовлявся надати запитувану інформацію, йому повідомляли, що така відмова *вплине на здійснення у подальшому соціальних виплат* [2].

З огляду на широкий резонанс та прискіпливу увагу суспільства до цього питання, важливим вбачається розгляд актуальних та проблемних питань обробки та захисту персональних даних в процесі верифікації соціальних виплат, пошук найоптимальніших шляхів врегулювання цих питань у вітчизняному правовому полі.

Метою статті є аналіз правових питань обробки та захисту персональних даних в процесі верифікації соціальних виплат, пошук шляхів подолання можливих негативних наслідків порушення приватності та інформаційної безпеки людини.

Виклад основного матеріалу. Аналіз правомірності обробки персональних даних з боку третіх осіб вимагає детального дослідження фактів такої обробки та їх правової оцінки.

Проте, насамперед, слід нагадати, що в цивілізованому світі вкладається в поняття “право на приватність”. Найбільш влучно позицію щодо необхідності захисту права на приватне життя людини зображують англо-американські дослідники цієї проблематики. Право на приватність, як вважає американський дослідник Рональд Холлборг, є “моральним принципом поваги до індивідуальної свободи” [5, с. 15]. У свою чергу, британський дослідник Артур Міллер зазначає, що “основною умовою для ефективної реалізації права на приватність є особиста можливість контролювати циркуляцію інформації, що стосується особи, яка є суттєвою для підтримання соціальних стосунків і особистих свобод” [6, с. 27]. Остання думка британського вченого є визначальною при формуванні підходів до захисту приватності людини.

Говорячи про аналіз правомірності обробки персональних даних з боку третіх осіб, звернемося до вже відомої, відкритої інформації, яка стала відома широкому колу громадськості, а також офіційних результатів позапланової перевірки офісом Уповноваженого Верховної Ради України з прав людини наведених фактів.

На підставі договору з Державним підприємством “Головний проектно-виробничий і сервісний центр комп’ютерних фінансових технологій” (Головфінтех) Міністерства фінансів України колекторська компанія ТОВ “Дельта М Юкрейн” отримала базу персональних даних громадян України. Відповідний договір підписаний за результатами двох виграних тендерів на проведення телефонної та фізичної верифікації (999 999 та 987 000 грн відповідно). У той же час, надані на запит ЗМІ роз’яснення Міністерства фінансів щодо передачі ТОВ “Дельта М Юкрейн” *лише ПІБ та номерів телефонів отримувачів соціальних виплат*, викликають багато питань.

Інформація, яку співробітники ТОВ “Дельта М Юкрейн” (за ініціативи Міністерства фінансів України!) використовували, є відомостями, за якими “*особа може бути конкретно ідентифікованою*”, тобто, відповідно до українського законодавства та міжнародного права, така інформація є “персональними даними”, які, в свою чергу, є невід’ємною складовою приватного життя людини та охороняються законом [7 – 9].

Після проведення позапланової перевірки, офісом Омбудсмена було встановлено, що ТОВ “Дельта М Юкрейн” надає послуги з проведення “телефонної верифікації” громадян на підставі договору з Державним підприємством “Головний проектно-виробничий і сервісний центр комп’ютерних фінансових технологій”. За умовами договору вказане підприємство передало ТОВ “Дельта М Юкрейн” базу даних “з дотриманням захисту персональних даних”. Разом з цим, доведено, що співробітники

ТОВ “Дельта М Юкрейн” у ході телефонних розмов просили уточнити у ВПО місце перебування таких громадян та іншу конфіденційну інформацію про особу, зокрема, *стосовно року народження, реєстрації місця проживання на непідконтрольній території та місця фактичного проживання* [3] .

Закон України “Про захист персональних даних” [7] встановлює вимоги до обробки та захисту персональних даних. Обробка персональних даних – будь-яка дія або сукупність дій, таких як збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення персональних даних, у тому числі з використанням інформаційних (автоматизованих) систем (стаття 2 Закону).

Обробка персональних даних здійснюється для конкретних і законних цілей, визначених за згодою суб’єкта персональних даних, або у випадках, передбачених законами України, у порядку, встановленому законодавством. Не допускається обробка даних про фізичну особу, які є конфіденційною інформацією, без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Мета обробки персональних даних має бути сформульована в законах, інших нормативно-правових актах, положеннях, установчих чи інших документах, які регулюють діяльність володільця персональних даних, та відповідати законодавству про захист персональних даних (стаття 6 Закону).

Поширення персональних даних передбачає дії щодо передачі відомостей про фізичну особу за згодою суб’єкта персональних даних. Поширення персональних даних без згоди суб’єкта персональних даних або уповноваженої ним особи дозволяється у випадках, визначених законом, і лише (якщо це необхідно) в інтересах національної безпеки, економічного добробуту та прав людини. Виконання вимог встановленого режиму захисту персональних даних забезпечує сторона, що поширює ці дані. Сторона, якій передаються персональні дані, повинна попередньо вжити заходів щодо забезпечення вимог цього Закону (стаття 14 Закону).

Крім цього, відповідно до статті 4 згаданого Закону, володільцем чи розпорядником персональних даних можуть бути підприємства, установи і організації усіх форм власності, органи державної влади чи органи місцевого самоврядування, фізичні особи-підприємці, які обробляють персональні дані відповідно до закону. Водночас, *розпорядником персональних даних, володільцем яких є орган державної влади чи орган місцевого самоврядування, крім цих органів, може бути лише підприємство державної або комунальної форми власності, що належить до сфери управління цього органу.*

Знову звернемось до результатів позапланової перевірки відповідно до законодавства. Встановлено, що на сьогоднішній день володільцем персональних даних, зібраних у процесі верифікації та моніторингу достовірності інформації, поданої фізичними особами для нарахування та отримання соціальних виплат, пільг, субсидій, пенсій, заробітної плати, інших виплат, що здійснюються за рахунок коштів державного та місцевих бюджетів, коштів Пенсійного фонду України, фондів загальнообов’язкового державного соціального страхування, є Міністерство фінансів України. Проте, розпорядником персональних даних внутрішньо переміщених осіб, володільцем яких є Міністерство фінансів України, наразі визначено юридичну особу приватного права – ТОВ “Дельта М Юкрейн”, що є порушенням вимог Закону України “Про захист персональних даних”. Всупереч вказаного закону було здійснено і передачу персональних даних внутрішньо переміщених осіб, які були зібрані Міністерством фінансів України в рамках процедури “верифікації і моніторингу” [3].

Отже, проаналізувавши вищенаведену інформацію, вбачається порушення цілої низки норм Закону України “Про захист персональних даних”, зокрема статей 2, 4, 6 та 14. Окрім цього, згадані порушення містять ознаки злочину, передбаченого статтею 182 Кримінального кодексу України (далі – КК України) [10]. Так, відповідно до статті 182 КК України незаконне збирання, зберігання, *використання*, знищення, *поширення конфіденційної інформації про особу* або незаконна зміна такої інформації, крім випадків, передбачених іншими статтями цього Кодексу, – караються штрафом від п’ятисот до однієї тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років.

У своєму відкритому зверненні Уповноваженим Верховної Ради України з прав людини було визначено: “…така ситуація є не лише кричущим випадком порушення права значної кількості осіб на недоторканність приватного життя, а й загрожує іміджу нашої держави на міжнародній арені. Адже однією з ключових умов повноправного входження України до європейського співтовариства є створення в нашій державі ефективного механізму захисту персональних даних, який би відповідав міжнародним стандартам у цій сфері” [3].

Стосовно негативних наслідків незаконного поширення персональних даних приватній компанії із сумнівною репутацією слід зазначити наступне. Так, аналітик Громадської організації “ОПОРА” О. Клюжев повідомив, що Міністерство фінансів передало ТОВ “Дельта М Юкрейн” усю інформацію, яку ВПО надавали при реєстрації: прізвище, ім’я, дата народження, телефон, місце проживання в анексованому Криму чи на окупованій частині території Донбасу, місце реєстрації на підконтрольній території, тощо. За його словами, це вже призвело до скорочення соціальних виплат [11]. Факти негативних наслідків наводять і інші громадські діячі , які визначають наступне [2]:

1. Порушення права громадян на захист персональних даних. Не дивлячись на публічну заяву Омбудсмана, Міністерство фінансів досі не надало жодних відомостей, які би давали мінімальні гарантії контролю за використанням вже переданих баз даних фізичних осіб. Як засвідчують звернення громадян на “гарячу лінію” (050 477 0800), будь-яка особа, яка дзвонить до колл-центру “Дельта М Юкрейн”, може фактично безперешкодно отримати персональну інформацію щодо іншого громадянина, маючи його номер телефону. Тому, крім самого факту неналежного використання державним органом персональних даних громадян є підстави вважати, що ці дані неналежно захищені і можуть використовуватися не за призначенням.

2. Порушення права на недоторканність приватного життя, яке вже відбулося після передачі даних третій стороні, додатково загострюється внаслідок проведеного тендеру на фізичну верифікацію. Згідно з додатком №3 до тендерної документації на закупівлю послуг з проведення фізичної верифікації, “метою збирання (звірки) інформації є перевірка особистих даних, місця проживання, місця праці фізичних осіб, фотографування місця проживання фізичних осіб для встановлення достовірності наданої ними попередньо інформації”.

3. Залучення компаній з управління заборгованостями до виконання державних функцій потенційно створює умови для психологічного насильства щодо громадян, враховуючи специфіку методів роботи колекторських компаній. Зокрема, на гарячу лінію ГО “Громадський Холдинг “Група Впливу” надійшло звернення жінки, яка повідомляла про те, що після її відмови спілкуватися з невідомими особами, оператори кол-центру дзвонили їй вісім разів протягом доби з різних номерів телефону, застосовуючи методи психологічного тиску.

4. Міжнародний характер діяльності групи компаній “Дельта М”, у тому числі на території Російської Федерації, створює ризики отримання нерезидентами України персональних даних громадян України з державних реєстрів. У випадку з внутрішньо переміщеними особами відповідна ситуація є особливо неприйнятною, враховуючи можливість проведення незаконної діяльності на окупованій та непідконтрольній території, зокрема щодо родичів та майна переселенців. Ця ж ситуація є неприпустимою щодо інших категорій громадян України, персональні дані яких можуть бути передані приватній структурі.

Варто зазначити, що проблеми практичної реалізації процедури “верифікації та моніторингу” достовірності інформації, поданої фізичними особами для нарахування та отримання тих чи інших виплат, набули системного характеру і пов’язані, перш за все, *з відсутністю належного законодавчого регулювання*. Нормативні акти, якими наразі врегульовано ці питання, мають відсилочний (бланкетний) характер стосовно ключових питань обробки персональних даних осіб, щодо яких проводиться верифікація. А це, у свою чергу, створює умови для безконтрольного доступу Міністерства фінансів України до персональних даних, що може спричинити безпідставне втручання у право особи на приватність.

Яскравим прикладом, яким створюється правова невизначеність питань обробки та захисту персональних даних у соціальній сфері в цілому, є прийняття Верховною Радою України Закону України “Про внесення змін до деяких законодавчих актів України” від 06.12.16 р. № 1774-VIII яким, серед іншого, вносяться зміни до частини 2 статті 13 Основ законодавства України про загальнообов’язкове державне соціальне страхування, зокрема до положення, у якому міститься заборона без згоди застрахованої особи розголошувати відомості про її страховий стаж, страхові випадки, результати медичних обстежень, суми одержуваних виплат тощо. Дану статтю доповнено словами “крім випадків, встановлених законом” та не враховується того, що випадки, за яких зазначені вище відомості можуть бути розголошені без згоди застрахованої особи, законом не визначені. Крім цього, згадана норма не узгоджується з одним із основних принципів регулювання інформаційних відносин, а саме з принципом захищеності особи від втручання в її особисте та сімейне життя (стаття 2 Закону України “Про інформацію”), та не враховує вимоги цього Закону, згідно з якими інформація про фізичну особу є конфіденційною і може поширюватися тільки за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов (частина 2 статті 21 Закону України “Про інформацію”) [12]. Така невизначеність і нечіткість норми може призвести до зловживань з боку державних органів та їх посадових осіб і ставить під сумнів у цілому захист персональних даних та право на таємницю приватного життя.

Висновки.

Комплексний аналіз проблемних правових питань обробки та захисту персональних даних в процесі верифікації соціальних виплат свідчить про необхідність інтенсивного пошуку підходів до їх вирішення державою, суспільством, науковим середовищем, простими громадянами нашої держави.

Пошук шляхів подолання можливих негативних наслідків порушення приватності та інформаційної безпеки людини в згаданому контексті має здійснюватись за наступними напрямками:

– усунення порушень права на недоторканність приватного життя, зокрема припинення незаконної обробки ТОВ “Дельта М Юкрейн” персональних даних внутрішньо переміщених осіб, шляхом впливу та чіткої взаємодії органів державної влади, Уповноваженого Верховної Ради України з прав людини;

– законодавче врегулювання повноважень державних органів України в рамках процесу верифікації та моніторингу достовірності інформації, поданої фізичними особами для нарахування та отримання соціальних виплат;

– внесення змін до чинного законодавства України з метою приведення законодавства у сфері соціального захисту громадян у відповідність до законодавства у сфері захисту персональних даних;

– прозоре розслідування фактів можливого незаконного поширення персональних даних з боку Міністерства фінансів України, незаконної обробки персональних даних ТОВ “Дельта М Юкрейн” компетентними правоохоронним органами нашої держави;

– широка інформаційно-роз’яснювальна робота працівників офісу Уповноваженого Верховної Ради України з прав людини серед державних службовців щодо правових питань обробки та захисту персональних даних.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-Вр // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – С. 141.

2. Відкрите звернення громадських організацій щодо передачі персональних даних фізичних осіб приватній колекторській компанії за публікацією А. Городецького на інформаційному ресурсі Донбасс SOS. – Режим доступу : http://donbasssos.org/02122016_kollek

3. Відкрите звернення Уповноваженого з прав людини щодо порушення права на недоторканність приватного життя Мінфіном. – Режим доступу : http://www.ombudsman.gov.ua/ua/all-news/pr/291116-xa-vidkrite-zvernennya-upovnovazhenogo-z-prav-lyudini-schodo-porush ennya

4. Про забезпечення прав і свобод внутрішньо переміщених осіб : Закон України від 20.10.14 р. № 1706-VII // Відомості Верховної Ради (ВВР). – 2015. – № 1. – Ст. 1.

5. Hallborg R.B. Principles of Liberty and Right to Privacy // Law and Philosophy. – 1986. – № 5. – P. 13-20.

6. Arthur R. Miller The Assault on Privacy. – Univ. of Mich. Press, 1971 – P. 25-32.

7. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI // Офіційний вісник України. – 2010. – № 49. – С. 199.

8. Про захист осіб у зв’язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.81 р. № 108 // Офіційний вісник України. – 2011. – № 1. – С. 701.

9. Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних : Директива Європейського парламенту і Ради від 24.10.95 р. № 95/46/ЄС. – Режим доступу : //www.zakon.rada.gov.ua/laws/show/994_242

10. Кримінальний кодекс України : Закон України // Відомості Верховної Ради України (ВВР). – 2001. – № 25 – 26. – Ст. 131.

11. Голова Комітету закликав Прем’єр-міністра України припинити беспрецендентне порушення прав вимушених переселенців – незаконну верифікацію. – (Новини Комітету Верховної Ради України з питань прав людини, національних меншин і міжнаціональних відносин). – Режим доступу : http://kompravlud.rada.gov.ua/kompravlud/control/uk/publish/article?art _id=56209&cat_id=45376

12. Про інформацію : Закон України від 02.10.92 р. № 2657-XII // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – Ст. 650 (у редакції Закону № 2938-VI(2938-17) // ВВР, 2011, № 32, ст. 313).

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

УДК 378.14.015.62

ДУБОВА С.В., *кандидат історичних наук,*
викладач Кафедри інформаційної, бібліотечної та архівної справи
Київського національного університету культури та мистецтв

ВІД МЕНЕДЖМЕНТУ ДОКУМЕНТНИХ ПОТОКІВ ДО МЕНЕДЖМЕНТУ ДЕРЖАВНИХ КОМУНІКАЦІЙ: РОЛЬ ДОКУМЕНТОЗНАВЦЯ В СУЧАСНИХ ОРГАНАХ ДЕРЖАВНОЇ ВЛАДИ

Анотація. *У дослідженні розглянуто роль та задачі документознавця в сучасних органах державної влади в межах оновленої концепції електронного урядування. Акцентовано увагу на тому, що раніше діяльність документознавців була достатньо чітко окреслена та відокремлена від таких процесів як “зв’язки з громадкісьтю”, однак в межах оновленої концепції електронного урядування вони дедалі більше стають нерозривною єдністю, яка забезпечує комунікування державних органів із суспільством. Наводиться міжнародний досвід (на прикладі Великобританії) щодо врахування в системі державної служби нових інформаційних реалій. Обґрунтовується необхідність переосмислення документознавців як фахівців з документних потоків на менеджерів офіційних державних комунікацій.*

Ключові слова*: документознавець, електронне урядування, комунікації, офіційні комунікації, менеджер офіційних державних комунікацій.*

Аннотация. *В исследовании рассмотрена роль и задачи документоведа в современных органах государственной власти в рамках обновленной концепции электронного правительства. Акцентировано внимание на том, что раньше деятельность документоведов была достаточно четко очерчена и отделена от таких процессов как “связи с общественностью”, однако, в рамках обновленной концепции они все больше становяться неразрывным целым, которое обеспечивает коммуницирование государственных органов с обществом. Приводится международный опыт (на примере Великобритании) относительно принятия во внимание в системе государственной службы новых информационных реалий. Обосновывается необходимость переосмысления документоведов, как специалистов по документным потокам на менеджеров официальных государственных коммуникаций.*

Ключевые слова*: документовед, электронное правительство, официальные коммуникации, менеджер официальных государственных коммуникаций.*

Summary. *The study examined the role and tasks of document specialist in modern public authorities within the revised concept of e-governance. The attention is drawn to the fact that previously the document specialist activities were delineated sufficiently clearly and separated from such processes as “public relations”, but within the revised concept of electronic governance they are increasingly becoming inseparable unity, which provides communication between the state authorities and society. An international experience (for example the Great Britain) is mentioned in relation to the incorporation of new information realities in the civil service. The necessity of rethinking of document specialists as experts of documentary flows to official government communications managers is justified.*

Keywords*: document specialists, electronic government, official communications, official government communications manager.*

Постановка проблеми. Сучасний розвиток інформаційних технологій вийшов за межі простого процесу інформатизації суспільства – тобто спрощення життя та життєдіяльності суспільства за рахунок автоматизації рутинної діяльності. Сьогодні це побудова нового типу суспільства, що має дедалі менше спільного із індустріальним,

а тим більш – аграрним. Процес вироблення, споживання інформації набув якісно нового значення, а найновіші технології (наприклад, такі як адитивні) взагалі роблять наше суспільство більше схожим на те, яким його уявляли 30 – 40 років тому.

Так само масштабними стали зміни у тих професійних сферах, які часто залишалися незмінними протягом десятиріч, а подекуди – століть. Особливо це стосується тих професій та фахових спрямувань, які задіяні в опрацюванні документних потоків у всіх їх проявах – діловодчі, архівні, управлінські, адміністративні загалом. Механічне збільшення цих потоків (зокрема їх кількості та якості), необхідність врахування все нових даних та параметрів, зростання кількості неструктурованої інформації (так званих “Великих Даних”) – все це формує принципово новий контекст діяльності інформаційних фахівців.

Не залишається осторонь цього процесу і державне управління. Процес розбудови електронного урядування, який на початку розглядався більшою мірою як допоміжний для державних службовців (на рівні автоматизації окремих процесів), сьогодні істотно вийшов за ці межі і набуває нового виміру та значення. Особливо це стосується комунікативної сфери держави, її взаємовідносин із суспільством та необхідності пояснювати суспільству свою діяльність та прийняті нею рішення. Стрімке зміщення акценту з державо-центричної до громадяно-центричної моделі держави відбувається передусім в сфері комунікування. Відтак, сама концепція державного управління все тісніше переплітається з загальними та спеціальними теоріями комунікації, а всі управлінські процеси розглядаються саме крізь призму комунікування.

Це стосується і документної складової державного управління. Якщо раніше вона була достатньо чітко окреслена та відокремлена від таких процесів як, наприклад, “зв’язки з громадськістю”, то в межах оновленої концепції електронного урядування вони дедалі більше стають нерозривною єдністю, які забезпечують комунікування державних органів із суспільством.

Це безпосередньо впливає на основні завдання, характер праці та особливості підготовки документознавців. В цьому контексті, власне, більш правильно ставити цілий комплекс питань про те, якою саме має бути їх підготовка та чим саме будуть займатись документознавці у цьому новому типі суспільства.

Ступінь наукової розробленості проблеми. Питання підготовки документознавців не залишаються поза увагою сучасних дослідників педагогічної науки і практики. Зокрема, слід відзначити дослідження передумов підготовки фахівців з документаційного менеджменту у вищих навчальних закладах України (Спрінсян В.Г.), формування професійних компетенцій майбутніх документознавців під час вивчення інформаційних дисциплін (Матвієнко О.В., Ліпінська А.В., Варенко В., Кушнаренко Н.М., Соляник А.А.), опрацювання міжнародного досвіду підготовки документознавців (Антоненко І.Є.), вивчення загальних питання документознавчої освіти (Морозюк І.І., Прокопенко І.П., Зозуля Н.Ю.), питання культури діловодства як механізму управління (Палеха Ю.І.). В контексті нашого дослідження важливими є також наукові студії, присвячені управлінському документознавству (Кулешов С.Г. та Бездрабко В.В.).

Метою статті є уточнення ролі та задач документознавця в сучасних органах державної влади.

Виклад основного матеріалу. Діловодча сфера і все, що пов’язане з офіційним (управлінським) документуванням, довгий час (і під “довгим часом” мається на увазі навіть не десятиліття, а століття) залишалось однією з найбільш консервативних та стабільних сфер управлінської діяльності взагалі. Наприклад, в Україні зародження діловодства сягає часів Київської Русі IX-XIII ст. [1]. Однак, сьогодні стрімко

змінюються самі умови життя соціуму. Ключова причина цього – становлення інформаційного суспільства або суспільства знань. Інформаційне суспільство стало причиною появи цілого комплексу альтернативних форм комунікування, як між окремими особами, так і між суспільством і державою. Наприклад: соціальні мережі, електронні приймальні, громадські ради, електронні петиції, масштабне становлення інститутів громадянського суспільства, глобальні процеси демократизації тощо. Це призвело до руйнування бюрократично-формалізованої монополії на комунікування, яка довгий час залишалась чи не єдиною моделлю взаємодії держави та суспільства. На противагу цьому формується новий довготривалий тренд плюралізації каналів комунікування, які сьогодні охоплюють меншою мірою формалізовані, однак, при цьому – офіційні канали взаємодії (а також подекуди неформальні канали взаємодії).

Наприклад, таким каналом, який на сьогоднішній день набуває дедалі більшої популярності, є інститут електронних петицій. З одного боку, електронні петиції мають офіційне визнання з боку державних органів, а подекуди – мають і практичні механізми їх імплементації. А з іншого – контроль за тими, хто безпосередньо користується цим механізмом, часто є суто формальним. Суть його проста: громадяни, попередньо зареєструвавшись та підтвердивши свої дані на сайті органу влади, збирають певну кількість підписів за ту чи іншу ідею, яку бажали б реалізувати. Відповідний орган влади реагує на таке звернення громадян у певні терміни. Так, для того, щоб у 10-денний термін Президент відповів на електронну петицію, потрібно, щоб вона зібрала 25 тисяч підписів протягом 3 місяців (90 днів). При цьому дедалі більше країн де такі механізми давно і успішно працюють – наприклад, в США та в багатьох європейських країнах.

Не є виключенням і Україна, наразі найпопулярнішим сервісом реєстрації електронних петицій є сайт Глави держави: за 11 місяців роботи на офіційному інтернет-представництві Президента було розміщено понад 21000 петицій від громадян. Триває збір підписів ще 2300 петицій [2]. Однак, крім президентського сайту з електронними петиціями, вже є і парламентський, і урядовий, і навіть на рівні місцевих адміністрацій.

Але повернемось до питання, яке винесено у назву дослідження: яким має бути місце документознавця в цій новій “системі координат”? Формально до останнього часу основною функцією документознавця в органах державної влади було управління документними потоками. Однак, якщо ми будемо чесними перед собою, то маємо визнати, що де-факто і у суспільній свідомості і у свідомості керівників державних інституцій документознавці майже завжди сприймалися як діловоди, а отже, як таких управлінських функцій майже не здійснювали. При цьому реально, навіть не зважаючи на це, документознавці завжди були задіяні в тій самій системі комунікування держави та суспільства (у вигляді документообміну – звернення громадян, відповіді на звернення, запити тощо) про яку йшла мова вище. Тобто, навіть здійснюючи свою безпосередню практичну функцію (створення, контроль, реєстрація, відправлення, зберігання документів), документознавець завжди був безпосереднім учасником широкого комунікативного процесу.

Однак, на даному етапі це питання суттєво ускладнюється тим, що широкі та масштабні процеси інформатизації можуть призвести до того, що саме безпосередня практична діяльність документознавців в органах державної влади може бути, якщо не знищена, то істотно нівельована. Це є одним з об’єктивних наслідків процесів інформатизації загалом, та створення системи електронного урядування зокрема. На

оперативному рівні це виражається у створенні одного з ключових елементів електронного урядування – систем електронного документообігу. Поширеною є аксіоматична думка (щоправда, переконливих підтверджень якої майже не має), що в “ідеальному випадку”і система електронного документообігу здатна повністю (або майже повністю) замінити фахівців, які безпосередньо задіяні у формуванні документного потоку організації. Це досягається за рахунок максимальної уніфікації документів, а також механізмів їх обробки. Наразі складно сказати, якою мірою цей прогноз може здійснитись найближчим часом. Однак, ігнорувати його цілком було б не доцільно, особливо зважаючи на ті здобутки інформатизації, які дозволяють автоматизувати не лише технічні та формалізовані процеси, але й в багатьох випадках творчі.

Концептуалізуючи зазначені вище тенденції, можемо узагальнити їх наступним чином: присутня висока ймовірність того, що внаслідок масштабних інформатизаційних процесів буде фактично знищено практичну сферу діяльності документознавців в органах державної влади, яка багато століть була і комунікативною сферою держави. На противагу цьому саме ця сфера істотно розширюється, перетворюючись на таке ж важливе завдання органу державної влади, як і його безпосередні функції.

В цих умовах документознавці можуть постати перед невблаганним вибором: або зникнути як професійна спільнота (мова йде саме про документознавців органів державної влади, однак не про інші галузі документознавчої сфери, наприклад – історичне документознавство), або переосмислити себе, як фахівців більш широкого профілю – *менеджерів офіційних державних комунікацій*.

На нашу думку, саме другий шлях є найбільш перспективним і доречним в сучасних умовах. Державні органи з кожним роком потребують дедалі більшої кількості фахівців, які, так чи інакше, пов’язані з комунікуванням у всіх його проявах. Яскравим прикладом цього є підхід, що був закладений у проект реформи державних комунікацій в Україні (підготовлений за допомогою донорської підтримки Уряду Великобританії [3]).

Дана реформа багато в чому ґрунтувалась на досвіді комунікативної реформи в самій Великобританії, яка здійснювалась з метою втілення ідеалів політичного нейтралітету британської державної служби та дотримання принципів об‘єктивності, достовірності урядової комунікації [4].

Особливу увагу у Великобританії приділяють професіоналізму працівників, що задіяні в безпосередній роботі зі ЗМІ та залучені до маркетингових проектів – професійні інформаційні службовці. Вони є державними службовцями, основною роботою яких є забезпечення вільного проходження повідомлень про політику до преси або через інші ринкові повідомлення.

У Британії є понад 1 000 професійних інформаційних службовців, які розподілені по всьому уряду. Їх обов’язки полягають у відповідях на запити преси, написанні прес-релізів з різних аспектів урядової політики, підготовці статей та повідомлень для газет та журналів, організації прес-конференцій та брифінгів для міністрів та вищих посадових осіб, наданні порад клієнтам. Вони також готують рекламні кампанії, керують виставками в межах країни та за кордоном, влаштовують публікацію урядової літератури.

Молоді фахівці при прийомі на роботу посідають найнижчий ранг кар’єрних сходів – помічник інформаційного службовця. Два перших роки в цьому ранзі є випробувальними. Новообрані працівники відвідують центри оцінювання, а потім просуваються на більш високий рівень – інформаційний службовець, переважно в інших міністерствах. Успішно просуваючись по кар’єрних сходах від одного міністерства до іншого на різних посадах, вони набувають професійного досвіду в усіх аспектах комунікативної роботи. Перш за все вони вивчають:

- як щодня працювати зі ЗМІ (сім днів на тиждень, 24 години на добу);
- як писати прес-релізи (близько 1 000 на рік), з тим щоб їх можна було відтворити в електронному вигляді в пресі з мінімальними змінами;
- як правильно давати поради найвищим посадовим особам;
- як визначати цінність новин;
- як досягти максимального впливу на цільові аудиторії [5].

Такий підхід – лише один з можливих щодо зміни профілю інформаційної роботи окремих державних службовців. Однак, в будь-якому разі комунікативна складова державної служби невпинно зростає, в тому числі – в Україні. Це можна побачити і з окремого рішення Уряду в межах впровадження нового Закону України “Про державну службу” і працівники прес-служб (комунікативних підрозділів) залишились державними службовцями (а отже тими, кого Уряд визнає вповноваженими здійснювати функції держави). На противагу цьому фахівці діловодних структур державних органів було визнано допоміжним (технічним) персоналом.

Однак, держава потребує не лише вузькоспеціалізованих фахівців з комунікацій, але й тих, хто здатен у всій повноті розуміння ситуації та комунікативного простору управляти (адмініструвати) всіма наявними комунікативними потоками та реагуванням на них. І саме документознавці могли б претендувати на цю складну та поліаспектну діяльність, яка потребує чітких організаційних навичок, здатності формалізувати результати діяльності та добру обізнаність із формальними (документними) аспектами діяльності державних структур. Фактично мова йде про перехід від управління документними потоками до управління офіційними державними комунікаціями.

Висновки.

Об’єктивний аналіз поточної ситуації вказує на те, що держава, відповідаючи на поточний виклик часу, робить “ставку” на розвиток власних комунікативних спроможностей та здатність ефективно комунікувати з суспільством. Це, в свою чергу, обумовлює необхідність і спільноті фахівців-документознавців осмислювати себе в цій новій реальності, а відтак і формувати адекватні вимогам часу пріоритети в галузі освіти.

На сьогоднішній день, ця вимога набуває особливого значення з огляду на те, що в межах перезатвердження Міністерством освіти України загального переліку спеціальностей, спеціальність “Документознавство та інформаційна діяльність” була ліквідована як самостійна і стала частиною новоутвореної спеціальності “Бібліотекознавство. Документознавство. Архівознавство”. Незважаючи на певну “стресовість” моменту, саме зараз час на глибинне переосмислення фаху та його освітнє наповнення. Якщо документознавці хочуть в цих нових умовах не просто залишитись конкурентноздатними, а взагалі просто залишитись затребуваними на ринку праці, плани підготовки молодих фахівців мають бути уточнені в частині збільшення дисциплін комунікативного циклу та аналітичної обробки інформації. Саме ці навички стануть будуть найбільш затребуваними, як у державному, так і у приватному секторі.

Підготовка документознавців має виходити з об‘єктивного стану сьогоднішніх та очікуваних найближчим часом потреб держави. А цією потребою є вміння не тільки і не стільки керувати документними потоками, скільки масштабно, швидко та ефективно використовувати всі наявні комунікативні можливості держави. І хоча навички управління документними потоками будуть ще вочевидь довго залишатись затребуваними та складати ядро документознавчої підготовки, але управління

офіційними державними комунікаціями має стати тим стратегічним орієнтиром в напрямку якого має модифікуватись та змінюватись підготовка документознавців для сфери державного управління.

Використана література

1. Кислюк К.В. Спеціальне документознавство : модульний курс / К.В. Кислюк. – К., 2011. – 192 с.

2. Рік електронного діалогу : чи є користь від петицій? – Режим доступу : http://www.slovoidilo.ua/2016/06/03/kolonka/aleksandr-radchuk/suspilstvo/rik-elektronnoho-dialohu-chy-ye-korys t-vid-petyczij

3. Презентовано концепцію реформи урядових комунікацій, розроблену Міністерством інформаційної політики України. – Режим доступу : http://www.kmu.gov.ua/control/publish/artic le?art_id=248775821

4. Інституційне забезпечення державної інформаційної політики : досвід країн Європи : аналіт. доп. – К. : НІСД, 2014. – 40 с.

5. Ефективна комунікація між державною службою та засобами масової інформації ; [пер. з англ. Л.Б. Магдюк, О.М. Рудік]. – Дніпропетровськ : Центр економічної освіти, 2000. – 68 с.

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

Правова інформатика

УДК 002.6:004:340.1+316.324.8

БРИЖКО В.М., *доктор філософії (Ph.D) з юридичних наук, с.н.с.*
ФУРАШЕВ В.М., *кандидат технічних наук, доцент, с.н.с.*

КОНВЕРГЕНЦІЯ НОВІТНІХ ТЕХНОЛОГІЙ: СТАН І ПЕРСПЕКТИВИ ЗМІН У ІНФОРМАЦІЙНИХ ВІДНОСИНАХ[*]

Анотація. *У статті досліджуються проблеми системної інтеграції новітніх інформаційних технологій, зокрема Інтернету речей, Хмарних технологій та Великих Даних, і перспективи змін у інформаційних відносинах.*

Ключові слова: *Інтернет речей, Хмарні технології, Великі Дані, конвергенція технологій, приватність, інформаційна безпека, інформаційне право.*

Аннотация. *В статье исследуются проблемы системной интеграции новейших информационных технологий, в частности Интернета вещей, Облачных технологий и Больших Данных, и перспективы изменений в информационных отношениях.*

Ключевые слова: *Интернет вещей, Облачные технологии, Большие Данные, конвергенция технологий, приватность, информационная безопасность, информационное право.*

Summary. *The issues of system integration of the newest information technologies are explored in the article, in particular those of the Internet of Things, Cloudy technologies and Big Data, as well as prospects of changes in the information relations.*

Keywords: *Internet of Things, Cloud technologies, Big Data, convergence of technologies, privacy, information safety, information right.*

Постановка проблеми. За останні декілька десятиліть істотно змінювалися як апаратна та операційно-програмна системи комп’ютера, так і обсяги накопичувачів даних. Спочатку користувачу доводилося взаємодіяти з важелями і перемикачами, потім прийшли чорні екрани с зеленим шрифтом і DOS, Macintosh від Apple і Windows від Microsoft, а потім і Інтернет з мобільною комунікацією та браузерами. Всі вони набували поступового поширення і сприяли змінам не тільки в уявленнях про інформаційну діяльність, але також, завдяки засобам електронно-інформаційного середовища, стали вносити істотні зміни в характер комунікації та нормативного упорядкування.

Новим значущим явищем, що впливає на зміни в інформаційній сфері, є поява та застосування різних у функціональному призначенні новітніх інформаційно-комп’ютерних та телекомунікаційних технологій. До основних з них можна віднести технології типу Інтернету речей та Хмарних технологій, які надають можливість зберігання, обчислювання та обробки значних обсягів даних завдяки так званих Великих Даних.

Сьогодні різноманітні технології, кожна з яких на початку створення передбачала конкретне функціонально-цільове призначення, застосовують можливості інших технологій, які інтегруючись стали доповнювати одна одну і у комплексі створювати, так би мовити, надсумарний ефект конвергентності та надавати нову якість результатів від сумісного їх використання.

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

Аналіз досліджень. Про результати аналізу проблем та перспектив новітніх технологій, погляди деяких зарубіжних та українських спеціалістів щодо їх впровадження, намагань юридичного визначення та правового упорядкування відносин, мова йде зокрема у [1 – 13]. Сама ж тема цієї роботи відносно нова, про що зазначається у [14]: “Конвергенція в інформаційній сфері як масове явище з’явилася в 90-і роки минулого сторіччя. В якості прикладів конвергенції продуктів, послуг і технологій можна привести наступні: користування електронною поштою за допомогою мобільних телефонів, доступ до телевізійних і радіопрограм за допомогою Інтернет-технологій, використання Інтернет-технологій для забезпечення голосової телефонії, використання комп’ютерів як пристроїв для прийому й відправлення текстових повідомлень, перегляду фільмів, прослуховування аудіозаписів, у якості кінцевого пристрою в IP-телефонії. У цілому, конвергенція принесла не тільки позитивні результати, але й ряд проблем: технологічні, технічні, економічні, комерційні й правові”.

В згаданій роботі увага приділена питанням, які виникають у сфері регулювання відносин щодо засобів масової інформації, на прикладі IPTV – цифрового телебачення, доступ до якого для користувачів здійснюється за допомогою Інтернет-технологій.

Сучасний стан Інтернет-сфери визначається становленням нової концепції телекомунікаційної мережі та технологій, яка отримала втілення у понятті-терміні “Інтернет речей” (скорочено IP, з англ. – Internet of Things (IoT)). Ця концепція завдяки Інтернету передбачає створення можливостей для системної інтеграції різних об’єктів-пристроїв (“речей”) між собою, кожний з яких покликаний здійснювати не тільки функціонування за призначенням, але й виконувати певні дії для взаємозв’язку з іншими об’єктами. Об’єкти-пристрої, які оснащені вбудованими процесорами та сенсорами, що підключені до Інтернету, набувають можливість інтероперабельності (здібності до взаємодії), тобто технологічного взаємнопов’язання між собою з метою обробки та обміну даними для виконання різних дій, у залежності від закладених в них програм, та без втручання людини, див., зокрема [1].

Поряд з “розумними” технологіями типу Інтернет речей, набувають поширення й інші ІТ-технології, так звані Хмарні обчислення або сервіси-послуги. Вони, в умовах збільшення обсягів інформації та завдяки Інтернет, надають можливості обробки, зберігання значних обсягів даних не на жорстких дисках комп’ютерів, а на віддалених серверах. Їх застосування є свідченням про черговий етап розвитку Інтернету, а разом з тим – про нові проблеми в сфері захисту приватності та інформаційної безпеки [15].

Нещодавно, у 2016 році, на конференції “Def Con” в Лос-Анджелесі обговорювались засоби захисту та безпеки у світі інформаційних технологій, який, як визначалося, продовжує стрімко удосконалюватися та змінюватися [16]. Експерти свідчили про технологічно-програмну уразливість практично всіх типів об’єктів-пристроїв, підключених до Інтернету. Програмні “діри” були знайдені у всьому – в “розумних” телепристроях, дверних замках, в сонячних батареях і термостатах, в автомобілях і в багато чому ін. Заражені гаджети за наказом хакера можуть здійснювати запити на будь-який IP-пристрій або веб-сайт, перенавантажуючи або блокуючи їх роботу. Раніше для цих цілей використовувалися комп’ютери, що працювали у режимі он-лайн. Пізніше до них приєдналися мережеві принтери, смартфони і інші пристрої, весь час підключені до Інтернету. Але зараз в таких атаках можуть брати участь навіть “розумні” лампочки, які технологічно пов’язані з іншими Інтернет речами. Як цього уникнути – однозначних рішень не визначено.

Таким чином, як постановка технологічних, так і юридичних проблем продовжує знаходитися у сфері дискусій та на початковому етапі пошуку шляхів їх вирішення.

Метою статті є узагальнення стану застосування та правового упорядкування інформаційних відносин у сфері новітніх технологій.

Виклад основних положень. Почнемо з поняття “Інтернет речей”. В одному з джерел воно пояснюється як “мережа різних об’єктів, що росте, – від промислових пристроїв до споживацьких товарів, які можуть обмінюватися інформацією і виконувати свої задачі, поки людина працює, спить або займається спортом. Інтернет речей складається з мільйонів датчиків і різних пристроїв, що генерують безперервні потоки даних, які можна використовувати для поліпшення як життя взагалі, так і для підвищення ефективності бізнесу зокрема” [17].

Інше джерело надає таке визначення: “Обчислювальна мережа з підключених до Інтернету об’єктів-пристроїв, які збирають, обмінюються даними та виконують відповідні функції за призначенням”[18].

Змістовний аналіз визначення “Інтернету речей” та авторський варіант дефініції, як правового терміна, надається у роботі [19]. Наводяться думки різних дослідників, деякі з яких, наприклад, вважають, що існує “обмеженість ряду визначень дефініції терміна “Інтернет речей” або технологічними, або функціональними аспектами, або аспектами, пов’язаними зі сферою використання IP”, та навіть те, що “загальноприйнятого визначення терміна “Інтернет речей” не існує”.

Американський дослідник М. Вебер має свою думку та зазначає, що: “…по суті, Інтернет речей означає різні речі для різних людей, в різних для них умовах і часі життєдіяльності. Одне з основних питань застосування Інтернет речей про те, як він працюватиме, як пристрої спілкуватимуться і ідентифікуватимуть один одного, як забезпечувати узгодженість з питаннями безпеки, захисту персональних даних і ін.” [3].

Як вважаємо, загально-технологічно (екосистемно) Інтернет речей із застосуванням Хмарних технологій схематично можна уявити наступним чином (див. Рис).

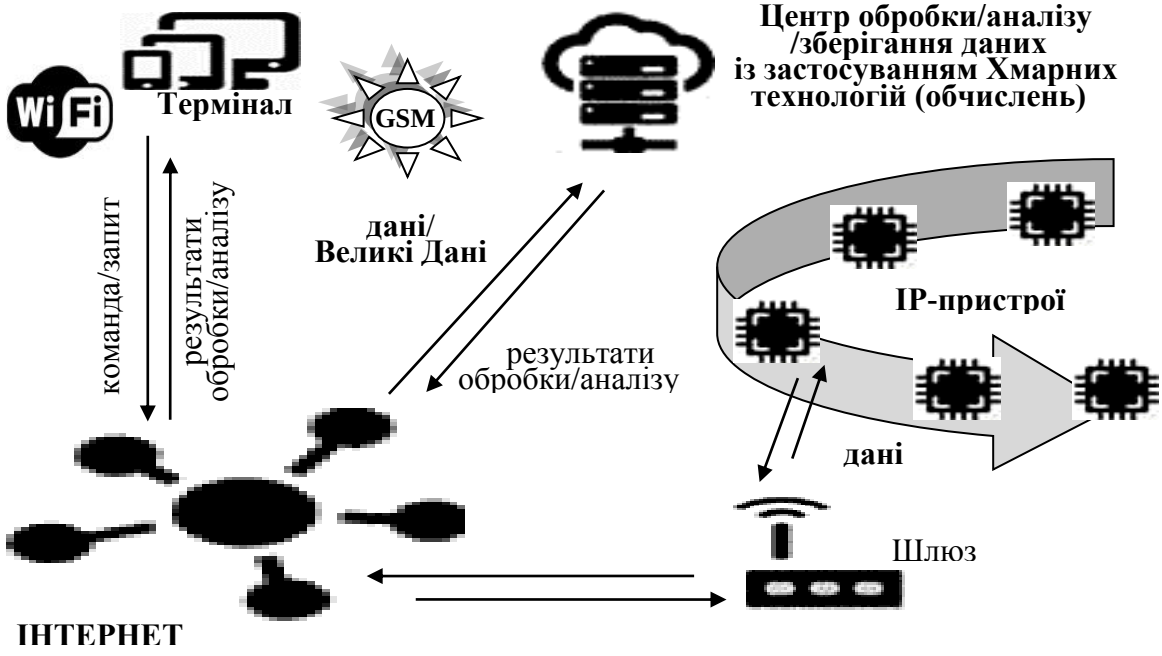

Рис.

Користувач використовує термінали (ноутбук, смартфон, планшет і т.п.) для відправки команд або запитів IP-пристроям безпосередньо через Інтернет або через Wi-Fi (стандарт “бездротової точності”) [20] на Інтернет, або завдяки GSM [21]. Пристрої

виконують команду щодо свого функціонального призначення та/або відправляють через Інтернет дані, які обробляються (аналізуються) і виводяться на дисплей терміналу в прийнятному для користувача вигляді. Дані можуть оброблятися та аналізуватися самими пристроями або центрами спеціалізованої обробки/зберігання даних, зокрема такими, які використовують Хмарні технології.

IP-пристрої, які визначаються як “розумні” (або “інтелектуальні”) об’єкти, надають можливості змінювати функціонування, наприклад, систем опалювання будинків, освітлення, роботу кондиціонерів, холодильників і багато ін. різноманітної техніки, що спрощує побутові проблеми та проблеми охорони здоров’я. Для підприємств IP-пристрої надають можливості контролю параметрів різних приладів, стану навколишнього середовища, логістики керування транспортом, енергозбереження [22]. Дедалі більше компаній починають надавати перевагу інтеграції новітніх технологій (рентабельність інвестицій, ефективність, продуктивність, зменшення різних витрат і т.д.) і, як вважається, корпоративний сегмент стане найбільшим ринком технологічного розвитку. Проте існує проблематичний момент – функціонуванням IP-пристроїв можна управляти дистанційно, у тому числі і сторонніми особами.

Для створення технологічного об’єднання різних об’єктів-пристроїв між собою завдяки Інтернет вважається за необхідне наявність таких основних умов, як [11]:

- для ідентифікації кожного об’єкту потрібна проста, компактна технологія. Тільки при наявності системи унікальної ідентифікації можна збирати та накопичувати дані про певний предмет. Такий функціонал можна забезпечити за допомогою чипів RFID (Radio-Frequency IDentification). Вони здатні без власного джерела струму передавати дані приладам зчитування. Кожен чіп має індивідуальний номер. Як альтернатива цій технології, для ідентифікації об’єктів можуть використовуватись QR-коди. З метою визначення точного місця його знаходження може використовуватися технологія GPS, яка використовується сьогодні у смартфонах та навігаторах;
- відстеження змін у стані об’єкту (або оточуючого середовища) може здійснюватися за допомогою сенсорів, якими вони мають бути оснащені;
- для обробки та накопичення даних з сенсорів також потрібно вбудовані в об’єкти мікропроцесори (чип-комп’ютер) ;
- обмін даними між об’єктами-речами може здійснюватися завдяки технологіям бездротових мереж (Wi-Fi[1], Bluetooth, ZigBee, 6LoWPAN).

Як зазначають у Львівському політехнічному інституті, основні роботи в області Інтернету речей ведуться за чотирма напрямками [11, с. 2]:

- розроблення технологій збору і обробки даних,
- розроблення технологій передачі даних,
- створення можливостей для пристроїв приймати самостійні рішення
- можливостей реалізації прийнятого рішення.

У аспекті нормативної політики щодо технологій в США. Сьогодні деякі з регулюючих органів, зацікавлених в розвитку впорядкування відносин, пов’язаних з Інтернетом речей, орієнтуються на нормативне регулювання за господарськими напрямами, тобто на фрагментарне регулювання конкретних питань по галузях [23].

[1] У статті “Wi-Fi йде в минуле” [http://invaders.com.ua/tech/5288] наводяться думки про те, що Wi-Fi, опинившись під натиском безлімітного мобільного Інтернету і більш сучасних технологій бездротової передачі даних, втрачає популярність, що може зробити його неактуальним в майбутньому.

Наявність безлічі стандартів, інтерфейсів і протоколів продовжує залишати багато відкритих питань з приводу застосування чинних законів. У зв’язку з цим не є видимими ознаки фактичної правотворчості або які-небудь конкретні напрями (правила) майбутнього нормативного регулювання. Залишається застосування існуючих стандартів, законів відносно провайдерів, конкуренції, інтелектуальної власності, захисту приватності і інформаційної безпеки. Проте, у матеріалах звіту Федеральної торгової палати США за 2015 рік, визначена думка про необхідність для сфери Інтернету речей спеціального законодавства [24].

В цей же час, для вирішення техніко-технологічних проблем, такі компанії як Microsoft, Intel, Qualcomm, Samsung, Electolux, Cisco і ін., створили об’єднану структуру “Відкрита структура взаємодії” (Open Connectivity Foundation, OCF). Її задачею є вироблення єдиних стандартів роботи і взаємозв’язку IP-пристроїв [25].

У контексті загальнодержавних планів, Голова Федеральної комісії по торгівлі США (FTC) Едіт Рамірес відзначає, що “Інтернет речей має великі перспективи для інноваційних споживацьких товарів і послуг. Але конфіденційність і безпека споживача повинні залишатися пріоритетом компаній, що розроблюють пристрої, які підключаються до Інтернету” [3].

Деякі аспекти Європейської політики щодо технологій. З 2010 р. Європейською Комісією в цілях розвитку розгортання технологій Інтернет речей проводиться дослідницька і консультантська робота з громадськістю, в якій участь в обговоренні беруть різні організації, а також представники держав-членів ЄС і третіх країн [26].

Як зазначалося у [1], у березні 2015 року був створений “Альянс для інновацій в Інтернет речей” (AIOTI), для формування інноваційної і промислової екосистеми європейського Інтернету речей. Метою AIOTI є створення конкурентного європейського ринку і нових бізнес-моделей IP. Стратегія передбачає необхідність уникати фрагментації і сприяти сумісності IP-пристроїв. За наслідками роботі на тій час Європейська комісія опублікувала робочий звіт “Просування Інтернету речей в Європі”, ґрунтуючись на трьох пріоритетах: процвітаючі IP-екосистеми, орієнтований на людину підхід до IP та єдиний ринок IP [27].

Ofcom – “Регулятор зв’язку Великобританії”, вже визначив деякі ключові сектори ринку IP – охорона здоров’я, транспорт і енергетика [28]. На цій базі передбачається формування основи системи додатків, з підтримкою існуючих пристроїв і мереж. Ринок пропонуватиме нові додатки, як по секторах, так і по країнах. Тому стоїть завдання вдосконалення комунікацій для забезпечення механізмів взаємозв’язку різних секторів шляхом технологічної сумісності IP, однозначної і надійної ідентифікації пристроїв, наявністю нового бездротового додаткового спектру роумінгу, а також підтримки політики інновацій в упровадження. Особлива увага концентрується на таких питаннях, як: сумісність стандартів IP, приватність та безпека, а також на рішення проблем аналітичної роботи з Великими Даними (див. далі по тексту).

Узагальнення положення справ та висловів, які в останні роки звучали в процесі численних дискусій і консультацій в США і ЄС, зводяться в основному до таких проблем, які потребують першорядного рішення.

Єдині стандарти. Передбачає розробку стандартів та ідентифікаційних протоколів шляхом інтероперабельності конкретних технологій на основі “відкритих систем”[2].

[2] В Україні у 1993 р. затверджений ДСТУ 2230-93. “Взаємозв’язок відкритих систем. Базова еталонна модель. Терміни та визначення” (ISO/IEC 2382-26:1993).

Сутність ідеологічної концепції єдиних стандартів передбачає інтеграцію максимальної кількості персональних і корпоративних електронних пристроїв в єдине інформаційно-функціональне поле. Забезпечити це без повної сумісності протоколів, інтерфейсів і системного софтверного змісту просто неможливо. Єдиним виходом для компаній, які бажають бути учасниками спільного глобального ринку електронних технологій, з максимально широким охопленням аудиторії споживачів послуг, стає вироблення єдиних стандартів і протоколів взаємодії. А це вимагає переходу від відособленості до максимальної відвертості [25].

Вважається, що технічні стандарти, в яких питання захисту даних належним чином вирішені, мають першорядне значення для взаємодії різних технологій. Відносно Інтернету речей, найпоширеніша думка полягає у тому, що існує необхідність у формуванні окремої платформи управління з участю зацікавлених сторін. Саме тільки стандарти можуть бути відповідним інструментом для цієї платформи. Одним з перспективних інструментів розглядається сертифікація.

Ідентифікатори. Застосовуються унікальні ідентифікатори для окремих IP (одноцільові) і індикатори для функціональної сумісності різних IP (багатоцільові). Останні надають можливість створення додатків багатофункціонального змісту, тим самим підвищуючи інтелектуальний рівень IP-взаємодії. Вони можуть в комплексі, до прикладу, допомогти в полегшенні у забезпеченні життя літніх людей в плані виявлення медичних проблем і їх профілактики, підтримки економності систем опалювання, водопостачання і освітлення будинку, здійснення регулювання роботи різних побутових приладів та ін. Разом з тим, при запевненні фірм-розробників IP про вигоди від IP-сумісності, які можуть бути досягнуті, поки мають місце досить технічних проблем і вартісних витрат. Складнощі у тому, що різні IP можуть відрізнятися альтернативністю і не достатньою взаємодією в підходах функціонування.

Важливою перевагою одноцільових ідентифікаторів є те, що вони підвищують рівень захисту приватності і безпеки.

Розподіл частотного діапазону. Вважається, що для інтеграції новітніх технологій потрібно поєднання бездротового і фіксованого зв’язку, а також використання мереж GSM, щоб передавати дані для взаємодії пристрою з пристроєм (M2M/IP, тобто Machine-to-Machine, – “машина-з-машиною”)[3]. Якщо пристрої отримають можливість “спілкуватися” між собою, головне при цьому те, щоб обмін даними не заважав їх основному функціональному призначенню. Є думка, що це має здійснюватися на основі встановлення частотних груп і ліцензування.

Антимонопольні проблеми. Включає пошук і створення умов об’єднання зусиль компаній в боротьбі з головною перешкодою на шляху розвитку взаємодії технологій – тотальною роздробленістю ринку і в одночасному прагненні домінування на ринку однієї технології, тоді як будь-яка з них може мати охорону згідно пропрієтарної теорії [25]. Це може свідчити про потребу вдосконалення охорони інтелектуальної власності і об’єктів ліцензування саме для сфери новітніх технологій.

Приватність та інформаційна безпека. У міру зростання кількості підключених до Інтернету об’єктів-пристроїв ростиме кількість потенційних загроз і можливих порушень. Інтернет речей, Хмарні технології, технології Великих Даних будуть збирати, обробляти, зберігати та поширювати величезні обсяги даних, причому в режимі M2M і без згоди суб’єкта даних, що може нести загрози порушення приватності та інформаційної безпеки.

[3] Дещо детально про M2M/IP, зокрема в Україні, див. [29].

Сьогодні є різні погляди на підвищення заходів приватності і безпеки для електронно-інформаційної сфери. Існує думка, що єдиного загального підходу в їх забезпеченні сформувати не уявляється можливим, і, отже, підходи повинні визначатися конкретними потребами у взаємопов’язаності і взаємодії різних технологій по галузях господарства. Хоча відомо, що будь-який взаємозв’язок між декількома пристроями і технологіями посилює не тільки потенційні техніко-технологічні проблеми, але створює додаткові складнощі в нормативно-правовому регулюванні.

Основи міжнародного законодавства для сфери персональних даних вже існують. Вони можуть бути прийнятними для безпосереднього застосування новітніх технологій. Головне питання полягає в тому, чи потрібне нове спеціальне законодавство або додаткові норми для Інтернету речей для забезпечення приватності і безпеки, і чи повинне воно бути м’яким (не завжди обов’язковим). Багато експертів вважають, що спеціальне ІР-законодавство може внести не тільки значні труднощі при його розробці і запровадженні, але також – швидко застарівати, у зв’язку з розвитком технологій. Проте, може мати значення введення окремих правових актів для ІР, а також розробка, наприклад, конкретних заходів для оцінки захисту даних, для ухвалення подальших рішень.

Найбільш поширена думка – конфіденційність за умовчанням повинна бути обов’язковою вимогою для ІР. Подальше вдосконалення захисту персональних даних в контексті загальної інформаційної безпеки має здійснюватися за рахунок того, що технології Інтернету речей не включатимуть особисту інформацію або ідентифікатори суб’єкта даних. Громадяни і організації повинні бути повністю обізнані про засоби контролю технологій і правила використання їх персональних даних. Забезпечення регулярного очищення зайвих даних вважається одним важливих чинників захисту.

В плані обов’язковості отримання інформаційного повідомлення про згоду суб’єкта права на використання його персональних даних, є думки про те, що із змінами обставин відповідні дані можуть не містити предмету конфіденційності, що вимагає необхідності врахування таких обставин.

Різними фахівцями і експертами також висловлюються припущення про те, що можливо з’являтимуться нові моделі у сфері безпеки, засновані на досвіді упроваджень новітніх технологій для вирішення нових задач. На відміну від тенденції, властивої споживацькому ринку Інтернету речей, де пріоритет швидкого отримання продукту коштує вище, ніж заходи безпеки, в корпоративному сегменті виробники рішень Інтернету речей повинні й надалі шукати баланс швидкості і безпеки [30].

У загальному плані забезпечення приватності та інформаційної безпеки повинне виходити з положень Доктрини інформаційної безпеки України від 25 лютого 2017 року № 47/2017, яка визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері [31]. В Доктрині, зокрема зазначається, що комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Етика, інформаційна та медійна грамотність. Етичні міркування є новою темою в контексті новітніх технологій. Вони, перш за все, стосуються питань захисту персональних даних, а саме: запобігання шкоді, контекстна їх цілісність (при перепрофілюванні) і моральної автономії (презентація самого себе). Є думки, що ІР може сприяти виникненню нових труднощів при дотриманні принципу контекстуальної

цілісності даних, згідно якому інформація, що надається для використання в одному контексті і з однією метою, може бути несанкціоновано використана іншими особами з іншою метою і в іншому контексті. Пріоритет призначеного для користувача елементу управління IP вимагає відповідності в захисті даних і прозорості в отриманні інформованої згоди від користувачів, що досягти буде не просто.

З розвитком технологій все більш звертають на себе увагу проблеми медійної та інформаційної грамотності. Міжнародна організація ЮНЕСКО опублікувала головні положення п’яти запропонованих нею правил-принципів (Laws of Media and Information Literacy, MIL), які розглядають ці дві сфери як комбінацію знань та навичок, необхідних сучасному суспільству в усьому світі. “Громадянам важливо розуміти функції медіа та інших джерел інформації, критично оцінювати їх контент, а також приймати обґрунтовані рішення – як користувачам, так і виробникам медіаконтенту та інформації”, – пояснюють в організації [32]. Принципи MIL охоплюють всі види ЗМІ та інші джерела інформації – бібліотеки, архіви, музеї та Інтернет, незалежно від використовуваних технологій. Особливу увагу передбачено приділити підготовці вчителів, щоб залучити їх до впровадження MIL в процес навчання, надання їм відповідних педагогічних методів, навчальних програм і ресурсів.

Цифрова грамотність. Існує думка, що нові технології сприяють збільшенню так званого “цифрового розриву”. Не всі можуть освоїти і користуватися інформаційними технологіями в рівній мірі. “Консиліум інформаційної економіки” [33], в плані підвищення цифрової грамотності і розширення масовості застосування нових технологій, закликає до побудови споживацької довіри у використанні даних, перш за все персональних даних. Для цього потрібен новий вид кваліфікованої робочої сили, яка не тільки знайома з принципами конвергенції новітніх технологій для надання послуг, зокрема Інтернету речей, і здатна підтримувати визначені мережеві для цього додатки, але і забезпечувати ефективний захист даних.

Зазначене напряму пов’язано з необхідністю в удосконаленні організації (програм) вищої освіти в Україні. Вже сьогодні вона потребує перетворень спрямованих на задоволення потреб в інженерах і вчених, чия діяльність буде пов’язана з технологіями Інтернету речей [11], а також з Хмарними технологіями [15] та Великими Даними [34]. Саме вони здатні об’єднувати різні програмні продукти, комплекси і об’єкти в єдину конвергентну систему.

Великі Дані. В останні роки у складі новітніх технологій набувають поширення так звані технології Великих Даних. Використання терміну “Великі Дані” (англ. – Big Data) відносять до Кліффорда Лінча, редактора журнала Nature, що підготував в 2008 році спеціальний випуск за темою “Як можуть вплинути на майбутнє науки технології, що відкривають можливості роботи з великими обсягами даних?”. В ньому були зібрані матеріали попередніх дискусій, що підсумовують роль даних в науці взагалі, в електронній науці, зокрема, а також про феномен вибухового зростання обсягів і різноманіття оброблюваних даних і технологічних перспектив в парадигмі вірогідного стрибка “від кількості до якості” [35].

Справедливості заради, слід згадати, що наявність проблеми “вибухового” зростання обсягів і різноманіття публікацій була визначена ще у 1945 році, коли керівник військової науки США Ванівар Буш вперше звернув увагу громадськості на проблему постійного значного збільшення їх кількості та обсягу. Він зазначив, що людину все більше приголомшує кількість та обсяги публікацій, які з’являються з такою швидкістю що їх неможливо ні усвідомити, ні тим більше запам’ятати. Тобто мова йде не лише про зростання великого обсягу відомостей, але про найбільш важливу

проблему, яка торкається всього процесу використання накопичених людством знань. Ця тенденція прискореного зростання відомостей у той час отримала визначення “інформаційного буму” або “вибуху” [36, с. 8].

Терміном “Великі Дані” прийнято описувати обробку великих масивів різноманітної інформації з складною, неоднорідною або взагалі невизначеною структурою. Ця інформація може бути структурована або неструктурована[4], проте повинна бути приведена до зручного у сприйнятті вигляду. Доктор технічних наук Д. Ланде у 2003 році констатував: “Не менш як 90 % інформації, з якою мають справу користувачі, є неструктурованою. Знайти щось цінне в ній можна лише за допомогою спеціалізованих технологій” [38].

Однозначного визначення “Великі Дані” немає. Кожен з спеціалістів трактує термін по-своєму. Згідно, наприклад, наданому у [39] – Великі Дані в інформаційних технологіях – це сукупність підходів, інструментів і методів обробки структурованих і неструктурованих даних величезних обсягів і значного різноманіття для отримання ефективних результатів, які сприймаються людиною, в умовах безперервного приросту, розподілу по чисельних обчислювальних вузлах мережі і альтернативним традиційним системах управління базами даних. Однак, для такого явища, як “Великі Дані”, крім місця для їх зберігання і комунікаційних каналів з величезною пропускною спроможністю, потрібно величезні обчислювальні потужності та аналітичні інструменти нового покоління [40]. Тобто, потрібна нова аналітика обробки даних, яка призначена для виявлення кореляцій, взаємозв’язків, але не причин, що є дуже важливим але, на жаль, у вище наданому визначенні мова про це не йде.

Застосування перших технологічних продуктів Великих Даних в інтересах не тільки економіки, але і політики, відносять до 2006 року [41]. З 2013 року наука про Великі Дані (англ. – Data Science) [42], як академічний предмет, вивчається за вузівськими програмами в США, які відображають питання, що лежать на стику інформатики, математики, статистики, прогнозування, економіки і бізнесу.

В якості джерел Великих Даних безперервно використовуються дані, що надходять з різних вимірювальних пристроїв, радіочастотних ідентифікаторів (RFID), соціальних мереж, мереж мобільного зв’язку про місцезнаходження абонентів, пристроїв аудіо- та відео реєстрації, метеорологічного і дистанційного зондування Землі і з безлічі ін. приладів, а також – з різноманітних баз даних. Вважається, що розвиток використання цих джерел ініціює проникнення технологій Великих Даних як в науково-дослідну діяльність, так і в сферу державного управління, а сам їх ринок буде одним з основних у сфері інформаційних технологій.

При цьому важливо зазначити, що сьогодні активно ведуться дослідження щодо внесення змін у способи зберігання даних.

Як повідомляє журнал Nature: зараз один біт в звичайних жорстких дисках займає близько мільйона атомів. Нещодавно міжнародна група фізиків-дослідників добилася граничної густини запису даних в магнітному стані речовини – один біт в одному атомі [43]. Це досягнення потенційно зможе змінити спосіб зберігання даних в майбутньому. Наголошується, що в дослідженні використовували гольмій, помістивши

[4] Неструктурована інформація – інформація, яка або не має наперед певної структури, або не організована в установленому порядку. Як правило, представлена у формі тексту, який може містити такі відомості, як дати, цифри і факти тощо. Це призводить до труднощів аналізу, особливо у разі використання традиційних програм, призначених для роботи із структурованими відомостями (анотованими або що зберігаються в базах даних) [37].

дані на один його атом: цей метал підходить для створення магніту з одного атома, оскільки містить багато неспарених електронів, що створюють сильне магнітне поле. До того ж, вони розташовані близько до ядра атома, тому захищені від зовнішніх дій.

Застосування технологій Великих Даних вимагає подальшого серйозного наукового і технологічного опрацьовування. Так, в Спеціальній доповіді компанії Gartner стверджується, що рішення задач Великих Даних включає більше, ніж просто зберігати та управляти великими обсягами даних. Перш за все це пов’язано з проблемою нових підходів до аналітики даних [44]. Її мета – мінімізація чинника людського втручання в підбір і обробку даних. Нова “Аналітика” будується за допомогою новітніх технологій і на основі відбору схожих тематик по кореляційних ознаках взаємозв’язку і взаємозалежності предметів, зіставленні різних рішень і продукуванні нових знань. Автори першої великої книги про Великі Дані стверджують: “Справжня революція полягає не в комп’ютерах, які обчислюють дані, а в самих даних і в тому, як ми їх використовуємо. …Володіння знанням, яке колись означало розуміння минулого, поступово перетворюється в здатність прогнозувати майбутнє” [45].

За прогнозами експертів, до 2020 року в Інтернет-просторі налічуватиметься близько 40 трильйонів гігабайт даних (результати наукових робіт, текстові повідомлення, відео-файли, аудіозаписи та багато ін.). Для орієнтації в таких обсягах необхідні технології, що мінімізують чинник людського втручання. Тому поява технологій Великих Даних припускає аналітичну революцію, що надасть можливість швидко і достовірно проводити автоматизований збір, фільтрацію, сортування, структуризацію і аналіз величезних обсягів даних [46]. Саме нова “Аналітика”, разом з такими елементами як “дані” і “технології”, є основою Великих Даних, яка і створює базове середовище для конвергенції будь-яких технологій.

Даних дійсно стає дедалі більше і більше, але при цьому залишається поза увагою та обставина, що проблема “інформаційного перенасичення” викликана не стільки збільшенням обсягів повідомлень, що з’являються в неймовірній кількості, скільки нездатністю старими методами впоратися з їх обробкою, розумінням та застосуванням знань, які вони надають. “Причина цього, – робить висновок російський учений Леонід Черняк – полягає, швидше за все, у тому, що за 65 років історії комп’ютерів так і не зрозуміло, що ж таке “дані” і як вони пов’язані з результатами обробки. Всі ці 65 років неймовірними темпами розвивалися власне технології роботи з даними і майже не розвивалася теорія інформації, що залишилася на рівні 50-х років, коли лампові комп’ютери використовувалися виключно для розрахунків. Ігноруванням ролі “даних” і “інформації”, як предметів дослідження, була закладена та сама міна, яка вибухнула зараз, в мить, коли змінилися потреби, коли рахункове навантаження на комп’ютери виявилося набагато меншим, ніж на інші види робіт з даними, а мета цих дій полягає в отриманні нової інформації і нових знань з вже існуючих масивів даних. От чому поза відновленням зв’язків ланцюжка “дані – інформація – знання” говорити про рішення проблеми Великих Даних безглуздо. Дані обробляються для отримання інформації, якої повинно бути рівно стільки, щоб людина могла перетворити її на знання” [35].

Далі Л. Черняк справедливо констатує: “За останні десятиліття серйозних робіт по зв’язках сирих даних з корисною інформацією не було, а те, що ми звично називаємо теорією інформації Клода Шенона, є не чим іншим, як статистичною теорією передачі сигналів, і до інформації, сприйманої людиною, не має ніякого відношення. Є безліч окремих публікацій, що відображають приватні точки зору, але немає повноцінної

сучасної (наукової – *від авт.*) теорії інформації[5]. В результаті переважна більшість спеціалістів взагалі не робить відмінності між “даними” і “інформацією”. При цьому, у науковому середовищі мають місце конструкції взагалі завуальованих дефініцій. Наприклад, у 2000 р. відомий учений у сфері правової інформатики, доктор юридичних наук, професор О. Гаврилов надає таке визначення: *“информацией являются используемые данные, представленные в форме, пригодной для передачи и обработки”* [48, с. 2].

Важливим наслідком, як ми вважаємо, є те, що вищезазначене сприяє такому стану справ, коли впродовж багатьох років новий науковий та юридичний напрям під назвою “Інформаційне право” не може отримати статусу окремої наукової спеціалізації, не кажучи вже про статус автономно-самостійної юридичної галузі.

Підтвердження вищевказаного можна знайти і в законодавчій базі України. Так, у ст.ст. 1, 6, 11, 13 – 15 Закону України “Про інформацію” від 13.01.11 р. № 2938-VI прямо вказується на те, що *“інформація” – це “дані…”*. З 1992 по 2011 рр. *під інформацією розумілися документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі*. А потім не тільки ця правова формула була змінена, але з Закону були вилучені формулювання стосовно “визначення інформації товаром” та “право власності на інформацію”. За результатами нормотворчості, базовий та рамковий Закон України для інформаційної сфери був ідейно перетворений на закон, який спрямований, перш за все, на забезпечення інтересів окремої галузі – масової інформації (тобто для окремого виду інформації; інше йшло лише як додаток до цього). Хоча було вже багато нормативно-правових актів, які мали безпосереднє відношення до діяльності журналістів (див., зокрема [49, с. 687]), і саме їх слід було лише доробляти. А Закон України “Про інформацію” – удосконалювати у плані товарного змісту “інформаційних ресурсів (продуктів)” та “персональних даних”, враховуючи умови поширення інформаційних технологій та ідею конвергенції інформаційно-технологічних процесів, яка на той час вже не лише проглядалася, але й пророблялася техніко-технологічно в розвинених країнах.

Проте, у ті ж часи, у ст. 3 Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” від 9 січня 2007 року № 537-V, було поставлено чітке та аргументоване завдання, зокрема: “*З метою підвищення ефективності розвитку інформаційного суспільства необхідно створити цілісну систему законодавства, гармонізовану з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснити кодифікацію інформаційного законодавства; …підготувати та прийняти Інформаційний кодекс України*”. На превеликий жаль визначені у Законі завдання, цілі та напрями розвитку інформаційного суспільства в Україні, за умов врахування змін у технологічних новаціях та міжнародного досвіду їх застосування, не отримали відповідного відгуку.

До речі, проблема методології та основ систематизації (кодифікації) інформаційного законодавства України досить детально досліджувалася (зокрема, див. [50]), але її рішення не отримало підтримки на реалізацію, оскільки, по-перше, це не вважалося за потрібне, а по-друге, передбачало залучення значних ресурсів (зокрема, значної кількості

[5] Першою спробою узагальнення світового досвіду щодо теорії інформації була книга “Основи наукової інформації”, яка була видана в 1965 р. Всесоюзним інститутом наукової і технічної інформації (див. [47]). Досить змістовний матеріал пояснював традиційні бібліотечно-бібліографічні методи і засоби роботи з документованою інформацією. Розглядалася тема автоматизації, але лише в частині пошуку документів. Проблема “дані – інформація” у той час не проглядалася, а автоматизація “Аналітики”, до того ж, не могла бути реалізована.

та обробки змістовного обсягу нормативно-правових документів України, ЄС та РЄ) та застосування для їх обробки не лише традиційних інформаційно-пошукових систем і баз даних, а перш за все – новітніх технологій з новою логікою обробки даних.

Сьогодні у багатьох фахівців існує впевненість в тому, що обробка Великих Даних неможлива без Хмарних обчислень. Поява Хмарних технологій не тільки у вигляді ідеї, а вже у закінчених і апробованих проектах, є початком розвитку аналітики Великих Даних. “Хмарні технології”, “Великі Дані” та нова “Аналітика” (точніше, аналітико-синтетична обробка даних та інформації – *від авт.*) – ці три чинника вектора в розвитку інформаційних технологій та інформаційного права, які не тільки взаємопов’язані, але вже не можуть існувати один без одного [44 – 46]. Саме вони складають *основний предмет перспектив системної інтеграції або конвергенції новітніх технологій, до яких можуть, за необхідності, бути залучені й технології типу Інтернету речей*.

Висновки.

1. Інформаційно-комп’ютерні технології сумісно з машиною-комп’ютером вже давно використовується не стільки як засіб, винайдений для прискорення розрахунків, а як електронно-інформаційний інструмент, який розширює можливості людини в обробці великої і різноманітної кількості даних, відборі інформації і прийнятті рішень на основі безлічі різних відомостей.

2. Завдяки сучасним методам та засобам, сьогодні створюються можливості і умови апаратно-технологічної інтеграції (конвергенції) різноманітних інформаційних технологій та ресурсів, що визначає не тільки в якому напрямі просувається розвиток електронно-технологічної сфери, але й потреби в трансформації поглядів на впорядкування інформаційних відносин. Це пов’язано з вирішенням нових та складних задач, які стосуються інформаційної безпеки, застарілих моральних проявів та корупції (яку лише технологічна автоматизація може реально зменшувати), регіональних і глобальних економічних моделей та, перш за все, – забезпеченням недоторканності приватного життя. Новітні технології, зокрема Інтернет речей, Хмарних обчислень та Великих Даних, складаються у конвергентне електронне середовище, яке стирає кордони у технологічних та правових обмеженнях щодо намірів збереження приватності, тим самим виявляючи неефективність існуючих як технічних, так і правових механізмів.

При цьому маємо думку, що конвергенція може активно наближати появу дійсно штучного інтелекту, безмежні можливості якого у створенні вже не новітніх, а когнітивно-машинних технологій не надають впевненості у тому, що все буде спрямоване на благо людини. В технологіях майбутнього лише сама людина буде себе захищати. Що з цього буде – відповідь не відома. Тому і треба займатися розробкою теорії наукової інформації, а не повторювати помилки історії прогресу.

3. В основу процесів конвергенції технологій закладається новий аналітичний підхід для отримання знань, який припускає мінімізацію чинника людського втручання. Нова “Аналітика” будується не стільки шляхом пошуку і відбору окремих відомостей або фактів по ключових словах (як в традиційних інформаційно-пошукових системах) з подальшими умоглядними висновками, скільки на основі підбору тематик за кореляційними ознаками взаємозв’язків і взаємозалежності предметів (об’єктів), зіставленні різних тематичних рішень (із залучення додаткових відомостей), прогнозуванні і продукуванні нових знань.

Ця “Аналітика” нагадує сучасну науково-технічну експертизу об’єктів промислової власності (патентне право), кожен з яких має чітке тематично-предметне визначення, завдяки Міжнародної класифікації винаходів. Для визнання будь-якої передбачуваної новації “винаходом”, експертиза порівнює і виявляє відмінності за істотними ознаками

формули винаходу не за одним прототипом (найближчим з декількох аналогів), а за сукупністю альтернативних рішень, і встановлює його відповідність “винахідницькому рівню”. Це найвищий рівень творчості, який визначається інтелектуальними здібностями у пошуку надсумарного ефекту спільного використання різних об’єктів. Саме цей критерій є свідченням появи наукової новини та нових знань. І тільки після цього видається охоронний документ – “патент”.

У сфері наукової та загально-технічної інформації (неструктурованої або слабко структурованою та з низькою точністю визначення індексів Універсальної десяткової класифікації або ключових слів, які лише позначають можливу область або області застосовування інформації), відтворити подібне того, як це здійснюється при експертизі об’єктів промислової власності, досить проблематично та вимагає багато трудоресурсів.

З зазначеного можна зробити такий важливий, на наш погляд, висновок – *відсутність чіткої структуризації інформації, а не “інформаційне перенасичення”, є головною проблемою у отриманні нових знань*.

Саме тому поява Хмарних обчислень та Великих Даних з новою “Аналитикою” стало дозволяти створювати умови конвергентно-аналітичної інтеграції в інформаційній сфері, завдяки можливостей швидко, більш предметно і повніше проводити автоматизований збір, фільтрацію, сортування, структуризацію і аналіз величезних обсягів даних та отримувати надсумарно-якісний ефект завдяки конвергентності технологій.

Більш того, у наш час вже поширюється думка про те, що виникнення умов конвергенції новітніх технологій є свідоцтвом взаємопроникнення світу матеріального та світу віртуального. І стає все важче зрозуміти, що ж не є “річчю”, якщо продовжувати залишатися на позиціях розділення світів і лише традиційного тлумачення матеріальності.

4. *Головний висновок*, який може виходити з вищесказаного, полягає у тому, що конвергенція новітніх технологій сприяє становленню Інформаційного права, як окремої автономно-самостійної галузі законодавства. Її основним завданням є створення умов гармонізації та збалансованості інформаційних відносин як в області загально-технічної інформації, так і в області інтелектуальної власності. Об’єктивно, зазначені області знань використовують один й той же предмет пізнання, який визначається поняттям “інформація”, а у правовому упорядкуванні та регулюванні відносин мають загальний предмет інформаційного права, який визначається словосполученням “інформаційні відносини”. Фактором підтвердження народження Інформаційного права як самостійної юридичної галузі може бути наявність Інформаційного кодексу, який, не відразу, але обов’язково почне створювати ту основу, на якій буде формуватися загальна гармонійність нормативно-правових приписів інформаційної сфери.

Здійсненню кодифікації інформаційного законодавства може передувати ухвалення адміністративного рішення про внесення у Перелік спеціальностей, за якими проводяться захист дисертацій, окремої спеціальності “Інформаційне право”. У науковій діяльності її базовими складовими є наукова, науково-технічна, науково-технологічна інформація та інтелектуальна власність.

Вже десятки років спеціалісти аргументують необхідність визначення Інформаційного права окремою юридичною галуззю, але, на превеликий жаль, численні дискусії мало що дають, відповідного владного рішення так і немає. Це, у загальному плані, можна розглядати як дивний фактор непорозуміння, який безпосередньо впливає на процеси розвитку інформаційно-правової сфери та розвитку інформаційного суспільства в Україні, про реальний стан яких, порівняно до інших країн, багато говорити не доводиться.

5. Нормативне рішення проблем взаємодії нових технологій вимагає всебічного аналізу як окремих технологій, так загальної інтеграційної картини їх застосування при доступі, обробці, обігу і забезпеченні захисту даних. Беручи до уваги значне коло проблем і зацікавлених сторін, узгодженість в багатьох питаннях не може швидко бути досягнута – сьогодні більше питань, ніж відповідей, тому дискусії продовжуються.

У плані міжнародного досвіду і загальних висновків, частково узгоджених за наслідками багатьох дискусій і консультацій останніх років, то вони зводяться до трьох проблем, яким передбачається надавати пріоритетну увагу, а саме:

- розробці технічних стандартів, системи ідентифікаторів і встановленню розподілу частотного діапазону. Це має найбільше значення для взаємодії технологічних систем;
- вдосконаленню європейської законодавчої бази і гармонізації правових стандартів захисту даних (жорсткіші заходи і зниження витрат) на основі єдиної моделі. Забезпечення захисту персональних даних за умовчанням (розглядається одним з основних напрямів при проектуванні і застосуванні технологій) і наявності згоди суб’єктів даних на їх збір різними пристроями. В даний час в США ретельно вивчається європейський досвід введення нових правових стандартів захисту персональних даних;
- вдосконаленню засобів забезпечення інформаційної безпеки, яке має ґрунтуватися на повазі до принципів та нормативних приписів міжнародного права.

6. В умовах подальшого та прискореного технологічного розвитку немає достатнього ступеня точності в тому, як вони розвиватимуться і які нові проблеми щодо захисту приватності та інформаційної безпеки держави виявляться в майбутньому. Це потребує нового погляду на більш предметне обговорення змісту консультацій з ІТ-спеціалістами та нормативно-правових дискусій стосовно підвищення ефективності системи захисту персональних даних в країні. Як вважаємо, в умовах поглиблення конвергентно-технологічних процесів та відсутності практичних рішень проблеми регуляції відносин в електронно-інформаційному середовищі, вказане не повинно виключати питання пошуку та застосування норм матеріального права до новітніх технологій і інформаційних ресурсів в контексті забезпечення захисту персональних даних, про що йдеться у [51].

Можливо слід брати до уваги характерний аспект функціонування традиційної організаційно-правової системи. В світі немає жодного органу (організації), який би відстежував факти порушення прав в сферах наукової, науково-технічної, науково-технологічної інформації та інтелектуальної власності (питання не торкається оперативно-розшукової або розвідувальної діяльності). Виявлення порушників і залучення їх до відповідальності – це проблеми самих зацікавлених осіб. Виходячи з того, що сучасні інформаційні технології дедалі більше ускладнюються і, в той час, мають спрямованість до функціонально-інтеграційного об’єднання, необхідним є пошук нетрадиційних юридичних рішень захисту прав людини у віртуальній сфері, зокрема захисту її природного права на персональні дані. Найважливіше з них може передбачати віднесення таких категорій як “дані” і “інформація” до об’єктів матеріального права в контексті додання їм статусу “товару”, який підпадає під регулювання пов’язаних з ним відносин в обсязі інституту “права власності”, на визначених законом умовах.

Використана література

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

2. Адам Тернер. Интернет вещей и носимые технологии : решение тайны частной жизни и безопасности, не сорвать инноваций. – 21 Rich. – JL & Технология. – № 6 (2015), – Режим доступу : http://jolt.richmond.edu/v21i2/article6.pdf

3. Mark Webber. The regulatory outlook for the Internet of Things. – (Posted on October 22nd, 2014). – Режим доступу : http://Users/Home85/AppData/Local/Temp/PART%202%20%E2%80%93%20The%20regulatory%20outlook%20for%20the%20Internet%20of%20Things%20%C2%AB%20Privacy %20and%20information%20law%20blog-1.html

4. The Societal Impact of the Internet of Things. A report of a workshop on the Internet of Things organized by BCS – The Chartered Institute for IT, on Thursday 14 February 2013. The Chairs were Jeremy Crump (BCS) and Ian Brown (Oxford Internet Institute, University of Oxford). – Режим доступу : https://www.bcs.org/upload/pdf/societal-impact-report-feb13.pdf

5. K. Rose, S. Eldridge, L. Chapin The Internet of Things : An Overview. Understanding the Issues and Challenges of a More Connected World / The Internet Society (ISOC). – October 2015. – 50 p. – Режим доступу : http://www.internetsociety.org/sites/default/files/ISOC-IP-Overview-2015 1022.pdf

6. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels, 28 October 2015. – Режим доступу : http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels

7. Eric Barbry. The Internet of Things, Legal Aspects: What Will Change (Everything) / Communications & Strategies, No. 87. – Pp. 83-100. – Quarter 2012. – Режим доступу : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2304137

8. Интернет вещей : всё подключается к сети. – Режим доступу : http://igate.com.ua/news/6309-internet-veshhej-vse-podklyuchaetsya-k-seti

9. Интернет вещей. – Режим доступу : //www.Users/Home85/AppData/Local/Temp/EPIC%20-%20%D0%98%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82%20%D0%B2%D0%B5%D1%89%D0%B5%D0%B9%20%28IoT%29.html

10. Будущее Интернета вещей, или как будут управляться огромные объемы данных. – Режим доступу : http://broadcast.net.ua/show/Infrastruktura/6155-buduweeinternetaveweijilikakbudutupravliatsiaogromnyeobemydannyh13.04.2016

11. Наконечний А.Й. Інтернет речей, захоплення чи перспективна технологія. – Режим доступу : //www.ir.lib.vntu.edu.ua/bitstream/handle/123456789/13105/ NAKONR...;

Програма Internet of Things у Львівській політехніці чекає абітурієнтів. – Режим доступу : http://itcluster.lviv.ua/programa-internet-things-u-l-vivs-kij-politehnitsi-chekaye-abituri yentiv

12. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека : сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

13. е-модели общественного устройства / [В. Брыжко, А. Орехов, О. Гальченко] : в кн. “е-будущее и информационное право”. – К. : Інтеграл, 2002. – 264 с. – С. 140-165. – (2-е вид. доп. та укр. мовою “е-майбутнє та інформаційне право” / [В. Брижко, Ю. Базанов, М. Швець, М. Коваль]. – К. : ТОВ “ПанТот”, 2006. – 234 с. – С. 96-115).

14. Баранов О.А. Правові проблеми конвергенції в інформаційній сфері // Правова інформатика. – 2009. – № 2(22). – С. 9-16.

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

16. Черний Р. Может ли Интернет вещей быть безопасным. – 2016 р., 10 серпня. – Режим доступу : http://igate.com.ua/news/16138-mozhet-li-internet-veshhej-byt-bezopasnym

17. Интернет вещей – аналитика вещей? – Режим доступу : http://channel4it.com/blogs/Internet-veshchey-analitika-veshchey-7403.html

18. Интернет вещей. – Режим доступу : http://igate.com.ua/news/15786-chto-takoe-internet-veshhej-infografika

19. Баранов О.А. Інтернет речей як правовий термін // Юридична Україна. – 2016. – № 5-6. – С. 96-103.

20. Wi-Fi – стандарт “бездротової точності”. – Режим доступу : http://www.broadband.org.ua/tekhnologii-bystrogo-interneta/1178-chto-takoe-wi-fi-printsipy-raboty -wi-fi

21. Global System for Mobile Communications. – Режим доступу : http://www.enetwtool.com/2014/02/24/cellular-technology

22. Promoting investment and innovation in the Internet of Things. Режим доступу : https://www.ofcom.org.uk/consultations-and-statements/category-1/iot

23. Internet of Things – Privacy and Security in a Connected World. – Режим доступу : https://www.ftc.gov/news-events/events-calendar/2013/11/internet-things-privacy-security-connected-world

24. Internet of Things : Privacy & Security in a Connected. – World Federal Trade Commission (FTC) Staff Report. – January 2015. – Режим доступу : https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IPrpt.pdf

25. Москалец А. OCF. Фундамент Интернета вещей? – Режим доступу : http://keddr.com/2016/02/ocf-fundament-interneta-veshhey

26. Internet of Things (IoT) merges physical and virtual worlds, creating smart environments. – Режим доступу : https://ec.europa.eu/digital-single-market/internet-things;

Conclusions of the Internet of Things public consultation. – (10th Meeting of the Internet of Things Expert Group. – Brussels, 14 November 2012. Tom Wachtel, rapporteur). – Режим доступу : https://ec.europa.eu/digital-single-market/news/conclusions-internet-things-public-consultation

27. Charlie Hawes. Hogan Lovells assists Internet of Things policy group in Brussels, 28 October 2015. – Режим доступу : http://www.hlmediacomms.com/2015/10/28/hogan-lovells-assists-internet-of-things-policy-group-in-brussels

28. Promoting investment and innovation in the Internet of Things, Ofcom, 23rd July 2014. – Режим доступа : https://www.ofcom.org.uk/consultations-and-statements/category-1/iot

29. M2M/IP. – Режим доступу : http://gagadget.com/21054-15-glavnyih-voprosov-o-tom-chto-takoe-m2m-i-pochemu-eto-interesno-kazhdomu

30. Интернет вещей : тенденции и прогнозы. – Режим доступу : http://hi-tech.ua/blog/internet-veshhey-tendentsii-i-prognozyi

31. Доктрина інформаційної безпеки України : Указ Президента України від 25.02.17 р. № 47/2017. – Режим доступу *:* http://www.president.gov.ua/documents/472017-21374

32. ЮНЕСКО визначила п’ять принципів щодо медійної та інформаційної грамотності. – Режим доступу : https://www.ukrinform.ua/rubric-society/2182980-unesko-viznacila-pat-principiv-medijnoi-ta-informacijnoi-gramotnosti.html

33. “Консилиум информационной экономики”. – Режим доступу : http://www.techuk.org/about/information-economy-council

34. Джозеп Курто. В будущем все компании будут использовать Big Data. – Режим доступу : http://ain.ua/dzhozep-kurto-v-budushhem-vse-kompanii-budut-ispolzovat-big-data

35. Леонид Черняк. Большие Данные – новая теория и практика // Открытые системы. СУБД. – М. : Открытые системы, 2011. – № 10. – Режим доступу : http://www.osp.ru/os/2011/10/13010990

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

37. Неструктурированные данные. – Режим доступа : https://ru.wikipedia.org/wiki/%D0%9D%D0%B5%D1%81%D1%82%D1%80%D1%83%D0%BA%D1%82%D1%83%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5

38. Ландэ Д.В. Добыча знаний. – Режим доступу : http://www.visti.net/~dwl/art/dz

Примітка. Про дослідження у сфері теоретичних і технологічних основ інтеграції інформаційних потоків в мережі Інтернет див. результати робіт доктора технічних наук, академіка Украинской академії наук Д.В. Ланде. – Режим доступу : http://dwl.kiev.ua

39. Великі Дані. – Режим доступу : https://ru.wikipedia.org/wiki/ %D0%91%D0%BE%D0%BB%D1%8C%D1%88%D0%B8%D0%B5_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D0%B5#cite_note-Gartner.E2.80.942011.E2.80.94.E2.80.94-5

40. Что означают термины “Большие Данные” и “Эра больших данных”? – Режим доступу : http://www.dailytechinfo.org/infotech/4276-chto-oznachayut-terminy-bolshie-dannye-i-era-bolshih-dannyh.html

41. Интернет проиграл эмоциям : почему технологии Обамы не спасли Клинтон. – Режим доступу : http://www.eurointegration.com.ua/rus/articles/2016/11/11/7057272/view_print

42. Big Data и Наука о данных. – Режим доступу : https://itsvit.org/our-services/big-data-and-data-science

43. Ученые смогли сохранить информацию в одном атоме. – Режим доступу : http://today-news.com/News/Technology/Uchenye-smogli-sohranit-informaciyu-v-odnom-atome-77063.html

44. Специальный доклад компании Gartner. – Режим доступу : http://www.gartner.com/patternbasedstrategy ; http://www.gartner.com/newsroom/ id/1731916

45. Майер-Шенбергер Виктор. Большие Данные. Революция, которая изменит то, как мы живем, работаем и мыслим / Виктор Майер-Шенбергер, Кеннет Кукьер. – М. : “Миф”, 2013. – 240 с. – Режим доступу : http://www.mann-ivanov-ferber.ru/books/paper book/big-data.PDF

46. Что такое Big Data. – Режим доступу : http://inlimited.com.ua/content/bigdata.php

47. Михайлов А.И. Основы научной информации / А.И. Михайлов, А.И. Черный, Р.С. Гиляревский. – М. : Изд. “Наука”, 1985. – 655 с.

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

49. Правове регулювання інформаційної діяльності в Україні ; упор. С.Е. Демський ; відп. ред. С.П. Павлюк. – К. : Юрінком Інтер, 2001. – 688 с.

50. БрижкоВ.М. Основи систематизації інформаційного законодавства : теоретичні та правові засади : монографія / В.М. Брижко. – К. : ТОВ “Пан-Тот”, 2012. – 304 с.

51. Pylypchuk, Volodymyr; Bryzhko, Valery; 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)

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

УДК 342.53:004.91

ДОРОГИХ С.О., старший науковий співробітник
НДІ інформатики і права НАПрН України

НАПРЯМИ РОЗВИТКУ СИСТЕМИ “ЕЛЕКТРОННОГО ПАРЛАМЕНТУ” В УКРАЇНІ

Анотація. *Розглядаються питання розвитку “електронного парламенту” в Україні.*
Ключові слова: *парламент, електронний парламент, бази даних нормативних актів.*

Аннотация. *Рассматриваются вопросы развития “электронного парламента” в Украине.*
Ключевые слова: *парламент, электронный парламент, базы данных нормативных актов.*

Summary. *The use and development of e-parliament in Ukraine.*
Keyword: *parliament, e-parliament, law databases.*

Постановка проблеми. Покращення рівня управління країною та залучення громадян до процесу законотворення є основною метою “електронної демократії”. Відповідно, впровадження новітніх інформаційно-комунікаційних технологій не є самоціллю без вирішення вказаної мети. Проте ці технології дозволяють значно розширити можливості по розбудові демократичного суспільства та побудувати інформаційні системи, спрямовані на організацію зворотного зв’язку, залучення фахового співтовариства та громадянського суспільства до законотворчого процесу, й врешті-решт підняти якість прийнятих законів.

При розгляді законотворчого процесу в першу чергу мова йде про побудову “електронного парламенту”. В широкому розумінні під “електронним парламентом” розуміють комплекс баз даних, програмного забезпечення та технічних засобів, створених для підтримки всіх стадій законотворчого процесу, забезпечення доступу громадян до публічної інформації та організації спілкування між громадянами, парламентом та депутатами.

Мета створення “електронного парламенту” полягає, передусім, у організації відкритої, прозорої діяльності законодавчого органу, що ґрунтується на взаємодії з громадянами і суспільством, забезпеченні їх участі у прийнятті законотворчих рішень та реалізується за допомогою засобів інформаційно-комунікаційних технологій [1, с. 3-4].

Побудова такої складної системи потребує вирішення цілої низки правових та організаційних питань, і розпочати необхідно з побудови загальної концепції.

Метою статті є представлення авторського погляду на модель “електронного парламенту” як системи, котра повинна не тільки являти собою внутрішню підсистему Верховної Ради України для забезпечення законодавчого процесу, але й бути піднята на вищий рівень, що включає побудову спільної системи в межах так званого “законодавчого трикутника”[1] та залучення громадянського суспільства та фахового співтовариства до законотворчого процесу.

Виклад основних положень. Згідно ст. 75 Конституції України [2] Верховна Рада України є єдиним органом законодавчої влади країни. Відповідно саме на Верховну Раду

[1] Під “законодавчим трикутником” розуміються суб’єкти законодавчої ініціативи згідно ст. 93 Конституції України, а саме Президент України, народні депутати України та Кабінет Міністрів України.

покладається організація законодавчого та законотворчого процесів, оприлюднення законів та ознайомлення усіх зацікавлених сторін із законопроектами, матеріалами пленарних засідань та роботи комітетів. Враховуючи потреби у обробці величезних обсягів інформації, пов’язаної із законотворчим процесом, виникла необхідність створення інформаційної системи, яка в подальшому могла не тільки забезпечувати інформатизацію законотворчого процесу, але й виконувати функції єдиної державної правової системи.

Першою спробою створення такої системи була Постанова Президії Верховної Ради України “Про організацію роботи по формуванню єдиної системи правової інформації в Україні” від 26.12.94 р. № 308/94-ПВ [3], яка зокрема містила положення про необхідність створення загальнодержавної системи правової інформації в Україні з метою підвищення рівня правотворчої і правозастосувальної діяльності органів державної влади, а також забезпечення найбільш сприятливих умов користування правовою інформацією громадянам, установам, організаціям і суб’єктам підприємницької діяльності в Україні. На виконання Постанови 308/94-ПВ була розроблена Концепція правової інформатизації [4, с. 49] та розпочаті роботи з інформатизації діяльності Верховної Ради України.

Результатом цих багаторічних робіт стала інформаційно-пошукова система Верховної Ради України, що розташована на веб-сайті Верховної Ради України та є єдиною повною безкоштовною державною базою даних нормативно-правових актів та законопроектів України. ЇЇ функціонуванням та розвитком опікується Апарат Верховної Ради України, згідно постанов Верховної Ради України та розпоряджень Голови Верховної Ради України, а саме: “Про затвердження Положення про Апарат Верховної Ради України” [5], “Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України” [6], “Про затвердження Положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет” [7].

В цілому система задовольняла вимоги інформаційного забезпечення законодавчого процесу у Верховній Раді України та інформуванню громадян щодо діяльності парламенту, проте розвиток інформаційно-комунікаційних технологій (далі – ІКТ) з одного боку й збільшення вимог щодо відкритості, підзвітності, прозорості та ефективності роботи парламенту потребує внесення змін як до концепції інформаційної діяльності парламенту, так і до його інформаційних систем, що забезпечують законотворчий процес.

Згідно дослідження, проведеного з ініціативи Міжпарламентського Союзу та Програми розвитку ООН і опублікованого у квітні 2012 року, парламенти стикаються з трьома домінуючими проблемами. Кожна із них проявляється в різний спосіб та з різною динамікою в різних країнах та регіонах. Але серед громадськості зростають спільні тенденції вимог. Ці тенденції такі:

– отримання більшого обсягу інформації про парламентську діяльність та про те, як на неї впливати;

– більша підзвітність парламентів та їх здатність реагувати на суспільні запити;

– отримання послуг відповідно до потреб громадян.

Відповідно для удосконалення інформування, роз’яснення та залучення громадськості вживається ціла низка різноманітних заходів. Ці заходи мають тенденцію розділятись на дві категорії:

– надання більшого обсягу інформації та покращення розуміння парламенту громадянами;

– збільшення консультацій з громадськістю [8].

У відповідь на вимоги, поставлені суспільством перед парламентом, була сформована концепція “електронного парламенту”.

Основними світовими тенденціями у розвитку “електронного парламенту” є впровадження новітніх ІКТ задля досягнення двох цілей: а) підвищити поінформованість громадськості та розуміння ролі парламенту в управлінні державою за допомогою надання громадянам інформації щодо його історії, функцій, процесів та дій, б) підвищити рівень активності громадян у процесі законотворення, залучаючи їх до участі у консультаціях, слуханнях, роботі комітетів та опитуваннях за допомогою технічних інструментів [9], тобто залучити громадян до системи побудови зворотного зв’язку у системі обговорення та виявлення проблем у сучасному українському законодавстві та спільному пошуку шляхів їх вирішення.

Важливість побудови зворотного зв’язку в системі державного управління і системі проходження інформації у структурах державної влади визначалась відомими вітчизняними фахівцями ще у 1990-х роках [10; 11]. У 2000 році Міжпарламентським союзом було розроблено Рекомендації [12] щодо змісту та структури парламентських веб-сайтів. У 2009 році ці Рекомендації було доопрацьовано та перевидано. Окремим розділом було визначено “Інструментарій комунікацій та діалогу з громадянами”.

На сьогодні ідеї розвитку “електронного парламенту” в Україні знайшли своє місце у “Програмі інформатизації законотворчого процесу у Верховній Раді України на 2012 – 2017 роки” [13] та у Доповіді та дорожній карті щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України [14], підготовленої Місією Європейського парламенту з оцінки потреб під головуванням Пета Кокса.

Програма передбачає, що створена 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 інформаційно-комунікаційних технологій із застосуванням високих стандартів доступу до інформаційних ресурсів парламенту [13]. В той же час Дорожня карта рекомендує посилити координацію між ініціаторами законодавства у Кабінеті Міністрів України, Адміністрації Президента України та Верховній Раді України та створити спільну систему електронного документообігу.

Ядром “електронного парламенту” є існуючі автоматизовані системи інформаційно-технологічного забезпечення діяльності Верховної Ради України, проте постає потреба у їх модернізації для більш широкого залучення громадського суспільства та наукового співтовариства до законотворчого процесу і побудови спільної системи електронного документообігу принаймні в межах “законотворчого трикутнику”.

Така спільна система електронного документообігу дозволить реєструвати законопроекти безпосередньо в Адміністрації Президента та Кабінеті Міністрів України і вже на цьому рівні стає можливим додавання до картки законопроекту експертних оцінок профільних міністерств та відомств та залучення громадських організацій та фахівців до аналізу законопроекту шляхом створення системи коментарів та обговорень.

На наступному етапі при проходженні законопроекту в парламенті необхідно забезпечити максимальну прозорість його проходження та обговорення як на рівні комітетів, так і на пленарних засіданнях. Стенограми (у подальшому, за технічної можливості, відео-файли) засідань комітетів та обговорення законопроектів у сесійній залі повинні відповідним чином індексуватись та пов’язуватись із законопроектом, що обговорювався, а також з депутатами, державними службовцями та науковими експертами, що вносили пропозиції щодо змін та доповнень. Також картка законопроекту повинна містити інформацію щодо результатів голосування. Тобто до

законопроекту в системі електронного документообігу повинна бути надана вичерпна інформація щодо його проходження, зауважень, експертних оцінок та його обговорень.

Окремо поовинна бути виписана процедура реєстрації та проходження законопроекту, отриманого шляхом електронної петиції або інших механізмів народного волевиявлення.

Прийнятий Закон, як й інші нормативно-правові акти, потрапляють до інформаційно-пошукової системи (далі – ІПС) “Законодавство”, котра не тільки виконує завдання не тільки забезпечення законотворчого процесу, але й виступає у якості єдиної в Україні безкоштовної ІПС нормативно-правових актів. Особлива роль ІПС “Законодавство” у тому, що на сьогодні це єдина державна повна інформаційно-пошукова система нормативно-правових актів України, що знаходиться у відкритому доступі через офіційний сайт Верховної Ради України за адресою http://rada.gov.ua.

В той же час існує ряд питань, пов’язаних з єдиною державною базою даних нормативно-правових актів, які необхідно вирішити. Так, на нашу думку, необхідно створити єдину електронну систему ведення нормативно-правових актів як на державному, так і на регіональному рівні. Необхідно розробити єдині формати ведення й обміну електронними документами у загальнодержавних, відомчих та регіональних правових базах даних, які би дозволили забезпечити громадянину вільний доступ до будь-якого нормативно-правового акту в країні, виключити дублювання витрат при розробці правових ІПС у кожному відомстві чи регіоні, що повинно значно зменшити витрати на розробку, підтримання й адміністрування відомчих й регіональних правових ІПС, полегшити доступ громадян до державних правових ресурсів та зробити прозорою діяльність органів влади.

Окремим важливим питанням постає механізм реалізації залучення громадян до законотворчого процесу. На сьогодні серед найперспективніших напрямів розвитку парламентських веб-сайтів, що надають змогу представити парламентську діяльність найбільш прозоро для громадян, належать технології веб-кастингу та впровадження системи комунікації між членами парламенту та громадянами шляхом створення блогів, дискусійних груп, форумів тощо, а також організації можливості коментування законопроектів.

Ці технології дозволяють досягти наступних цілей:

– підвищити поінформованість громадськості та розуміння ролі парламенту в управлінні державою за допомогою надання громадянам інформації щодо його історії, функцій, процесів та дій;

– підвищити рівень активності громадян у процесі законотворення, залучаючи їх до участі у консультаціях, слуханнях, роботі комітетів та опитуваннях за допомогою технічних інструментів.

Необхідно відзначити потребу у комплексності побудови всіх залучених ресурсів, коли при ознайомленні із законопроектом можна було б не лише відслідковувати стадії його проходження, знайомитись з основним текстом, внесеними правками, висновками науково-експертного управління Верховної Ради України, але й мати можливість переглянути відеозапис представлення й обговорення законопроекту в сесійній залі (за можливості і в комітеті), ознайомитись з громадським обговоренням і думками незалежних фахівців за цією тематикою.

Висновки.

Для реалізації цілей “електронного парламенту” пропонується створення інтегрованої бази даних законотворчого процесу у Верховній Раді України (інтегрованої інформаційно-комунікаційної системи Верховної Ради України та моделі взаємодії між

її складовими, моделі інтеграції сервісів баз даних законотворчого процесу з автоматизованими системами Верховної Ради України: “електронною залою” пленарних засідань, “електронним офісом” народного депутата України, “електронним комітетом”, “електронною Погоджувальною радою”, “електронною бібліотекою”, єдиним веб-порталом Верховної Ради України, веб-сайтом Голови Верховної Ради України та веб-сайтами комітетів) із забезпечення реалізації повноважень Верховної Ради України.

В подальшому пропонується розширити систему “електронного парламенту” шляхом побудови спільної системи електронного документообігу із Адміністрацією Президента та Кабінетом Міністрів України як складової “законодавчого трикутника” та побудувати систему зворотного зв’язку з громадським суспільством та фаховим співтовариством.

Перспективи щодо подальших досліджень полягають в розробці нової концепції законотворчого процесу “від початку до кінця” в напрямах організації проходження законопроекту через систему єдиного електронного документообігу в межах “законотворчого трикутника”, розроблення процедури залучення громадян, наукового співтовариства та експертних структур органів виконавчої та судової влади до законотворчого процесу, організації систем електронного документообігу та залучення громадськості до нормотворчого процесу на рівні місцевого самоврядування.

Використана література

1. Маруженко О.П. Інформаційне забезпечення законотворчого процесу в Україні: дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.07 / Олексій Петрович Маруженко ; Інститут законодавства Верховної Ради України. – К., 2009. – 233 с.

2. Конституція України : Закон України від 28.06.96 р. // Відомості Верховної Ради (ВВР). – № 30. – Ст. 141.

3. Про організацію роботи по формуванню єдиної системи правової інформації в Україні : Постанова Президії Верховної Ради України від 26.12.94 р. № 308/94-ПВ. – Режим доступу : http://zakon.rada.gov.ua

4. Інформатизація законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності : посібник / [Горьовий Л.Є., Швець М.Я., Дрогаль Т.Г. та ін.]. – К. : Парламентське видавництво, 1999. – 199 с.

5. Про затвердження Положення про Апарат Верховної Ради України : Розпорядження Голови Верховної Ради України від 25.08.11 р. № 769. – Режим доступу : http://zakon.rada.gov.ua

6. Про Перелік автоматизованих систем інформаційно-технологічного забезпечення діяльності Верховної Ради України : Розпорядження Голови Верховної Ради України від 01.07.03 р. № 663. – Режим доступу : http://zakon.rada.gov.ua

7. Про затвердження Положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет : Розпорядження Голови Верховної Ради України від 24.05.01 р. № 462. – Режим доступу : http://zakon.rada.gov.ua

8. Global Parliamentary Report : The changing nature of parliamentary representation / Inter-Parlamentary Union ; United Nations Development Programme. – 2012. – Mode of access : http://www.ipu.org/gpr

9. Світовий е-парламент : Звіт 2012. – Режим доступу : http://pdp.org.ua/images/stories/materials/GLOBAL_E-parlament_Report_2012_ukr.pdf. – (Глобальний центр з питань ІККТ у парламенті).

10. Інформатизація законотворчої, нормотворчої, правозастосовної та правоосвітньої діяльності : посібник. – К. : Парламентське видавництво, 1999. – 199 с.

11. Комп’ютеризована система інформаційно-аналітичного забезпечення законотворчої та правозастосовної діяльності: посібник. – К. : Парламентське видавництво, 1998. – 149 с.

12. Guidelines for Parliamentary Web sites. – Inter-Parlamentary Union, 2009. – Режим доступу : http://www.ictparliament.org/sites/default/files/webguidelines_en.pdf

13. 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. – Режим доступу : http://zakon.rada.gov.ua

14. Доповідь та Дорожня карта щодо внутрішньої реформи та підвищення інституційної спроможності Верховної Ради України. – (Підготовлена Місією Європейського парламенту з оцінки потреб під головуванням Пета Кокса, Президента Європейського парламенту 2002 – 2004 (вересень 2015 – лютий 2016) ; Європейський парламент, 2016. – Режим доступу : http://www.europarl.europa.eu/resources/library/media/20160301RES16508/20160301RES16508.pdf

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

Інформаційна і національна безпека

УДК 316 (477)

ДЗЬОБАНЬ О.П., *доктор філософських наук, професор,* головний науковий співробітник НДІ інформатики і права НАПрН України
МАНУЙЛОВ Є.М., *доктор філософії, професор,* професор кафедри філософії Національного юридичного університету імені Ярослава Мудрого

ІНФОРМАЦІЙНА БЕЗПЕКА В КОНТЕКСТІ ІНФОРМАЦІЙНОЇ КУЛЬТУРИ

Анотація. *Показано, що ключовим фактором ризику для інформаційної підсистеми соціуму виступають масштабні соціокомунікативні та соціокультурні трансформації, що несуть у собі низку негативних соціальних наслідків. Продемонстровано, що в останні роки чітко фіксуються дезорганізаційно-дисфункційні тенденції, безпосередньо пов’язані з високими швидкостями інформаційних змін. Обґрунтовано, що стан інформаційного перевантаження призводить до виникнення різних проблем, пов’язаних із забезпеченням інформаційної безпеки як самого суб’єкта, так і наявної у нього інформації.*

Ключові слова: *інформаційне суспільство, інформаційна культура, інформаційна безпека, інформаційна сфера, інформаційні технології.*

Аннотация. *Показано, что ключевым фактором риска для информационной подсистемы социума выступают масштабные социокоммуникативные и социокультурные трансформации, которые несут в себе ряд негативных социальных последствий. Продемонстрировано, что в последние годы четко фиксируются дезорганизационно-дисфункциональные тенденции, непосредственно связанные с высокими скоростями информационных изменений. Обосновано, что состояние информационной перегрузки, приводит к возникновению различных проблем, связанных с обеспечением информационной безопасности как самого субъекта, так и имеющейся у него информации.*

Ключевые слова: *информационное общество, информационная культура, информационная безопасность, информационная сфера, информационные технологии.*

Summary. *It is shown that a key risk factor for the information subsystem of society is major socio-communicative and sociocultural transformations that carry the row of negative social consequences in themselves. It is shown that disfunctional trends direct-coupled with high-rate of information changes were clearly recorded the last years. It is reasonable that the state of information overload results in the the different problems related to providing of information safety of both subject and information held by him.*

Keywords: *information society, information culture, information safety, information sphere, information technologies.*

Постановка проблеми. Необхідність в осмисленні проблеми безпеки соціальних суб’єктів пов’язана з характерним для сучасності зростанням інтенсивності інформаційних потоків. У філософському пізнанні виникають нові завдання, пов’язані з приведенням методологічних засобів філософської науки у відповідність із світоглядною парадигмою нестабільності сучасного світу й розумінням того, що зростання інформації – це і необхідна умова у функціонуванні та розвитку соціальних систем, і значна загроза для суспільства.

На даному етапі розвитку людства соціальний суб’єкт вступив у нову фазу, де основним предметом праці є інформація і знання, знаряддям праці – інформаційні технології та засоби комунікації, а саме суспільство поступово стає інформаційним.

Звернення суспільної свідомості до проблем інформаційної безпеки пов’язано з новими особливостями життя у сучасному суспільстві. Скорочуються соціальні практики аграрного та індустріального виробництва – вони технологізуються, стають інтелектуально й інформаційно насиченими. Дедалі більша частина суспільства втягується в роботу з інформацією, інформація стає найважливішим ресурсом суспільства. Поряд з поняттями “промислова індустрія”, “інфраструктура промисловості” дедалі частіше в діловій мові ми зустрічаємо поняття “інформаційна індустрія”, “інформаційна інфраструктура”.

Для наступаючої інформаційної епохи характерна специфічна форма соціальної організації, в якій нові інформаційні технології стають фундаментальним джерелом продуктивності і влади (М. Кастельс [1]). Сьогодні будь-яка соціальна практика, особливо пов’язана з виробництвом і управлінням у широкому сенсі цього слова, актуалізує певний спектр інформації й обумовлена проблемою інформаційної безпеки.

Наростання складності, багатоаспектності соціального життя, зростання швидкості його перебігу пов’язані зі зростанням інтенсивності інформаційних процесів у суспільстві і зростаючою швидкістю старіння інформації. Подібна ситуація викликає до життя нові ризики й загрози, одночасно примножуючи колишні. Ризики й загрози є основними параметрами, за допомогою яких прогнозуються й вирішуються будь-які соціальні проблеми, чи то державне управління, пов’язане з постійним реформуванням соціальних структур, або соціально-економічні рішення, що приймаються різними іншими соціальними суб’єктами. Безпека суб’єкта, як і безпека системи суспільства в цілому, формується наявністю/відсутністю інформації та зростаючою швидкістю старіння інформації. Причиною і того, й іншого є зростання інтенсивності комунікацій в суспільстві [2 – 4].

Сьогодні становлення інформаційного суспільства в усьому світі залежить від безлічі різних факторів, серед яких одним з найважливіших є його інформатизація. Сучасний етап інформатизації суспільства можна охарактеризувати наступним чином: з одного боку, відбувається бурхливе зростання інформації (тобто її виробництво й накопичення) за кількісними та якісними показниками, з іншого боку, суб’єкт інформаційних відносин (людина, суспільство) не здатний за короткий термін обробити весь обсяг повсякденної і наукової інформації, що надходить до нього. Внаслідок цього настає стан інформаційного перевантаження, що призводить до виникнення різних проблем, пов’язаних із забезпеченням інформаційної безпеки як самого суб’єкта, так і наявної у нього інформації.

Результати аналізу наукових джерел і публікацій свідчать, що незважаючи на достатньо суттєве опрацювання проблеми інформаційної безпеки у різноманітних її проявах, єдності у розумінні сутності даного феномена у сучасній науковій парадигмі немає. Узагальнююче філософське осмислення даної проблеми в контексті інформаційної культури теж, на жаль, знаходиться не на належному рівні.

Метою статті є подальше опрацювання сутності феномену інформаційної безпеки в контексті інформаційної культури.

Виклад основного матеріалу. Сучасне суспільство поступово стає дедалі більш інформаційним, не тільки через те, що воно насичується інформацією та інформаційними технологіями, а й тому, що його соціальний і економічний розвиток залежать від володіння адекватною інформацією та від уміння правильно користуватися

нею. Головну роль у такому суспільстві відіграє інформація, причому точна, доступна і своєчасна. На цій підставі інформація перетворюється на третій вид ресурсів, поряд з речовиною і енергією. Все це веде до того, що в усьому світі відбувається поступова інформатизація суспільства.

Як справедливо стверджує О. Маркозова, “інформаційне суспільство і його система цінностей є не тільки благом, що сприяє становленню самостійної особистості, розвитку її внутрішніх ресурсів, але й несе загрозу традиційним цінностям і культурі і сучасна цивілізація стрімко трансформується у “суспільство ризиків”, яке ускладнює процеси життєдіяльності людини” [5, с. 179].

У міру освоєння інформаційної сфери, людина на своєму шляху зустрічає певні труднощі, деякі з яких їй доводиться вирішувати самостійно. Це призводить до проблеми формування у суб’єкта інформаційної культури, від рівня якої залежить здатність людини адекватно реагувати на зміни, що відбуваються навколо неї [6; 7].

Якщо спробувати коротко охарактеризувати поняття “інформаційна культура”, то можна сказати, що воно містить в собі узагальнення, які стосуються інформаційних знань, умінь і навичок людини, її здатності працювати з інформацією тощо [6; 8]. Інформатизація та розвиток інформаційних технологій впливають на формування інформаційної культури суб’єкта (людини, суспільства) і якісно визначають її склад і властивості.

Сьогодні, в умовах “інформаційного вибуху”, на перше місце виходить уміння користуватися інформацією, а засвоєння знань відходить на другий план, що впливає на всю структуру системи освіти і на підготовку суб’єктів для роботи у будь-якій сфері. Таким чином, що вищий рівень інформатизації та інформаційної культури суб’єкта (людини, суспільства), то менше виникає проблем, пов’язаних із забезпеченням інформаційної безпеки.

Сучасні темпи розвитку інформаційних технологій перевершили всі очікування і спростували навіть найсміливіші прогнози. Справа в тому, що окремі підсистеми обробки інформації (операційні системи, мережі) розвиваються швидше, аніж інфраструктура, в якій їм визначено працювати. Можливості апаратури зростають зараз набагато швидше, аніж очікувалося в численних прогнозах десятирічної давності. Досить згадати, що обсяг дискової пам’яті сьогодні кожні три роки збільшується в чотири рази, а ємність оперативної пам’яті подвоюється не щороку, як було ще недавно, а кожні шість місяців. В результаті відповідна інфраструктура, яка будувалася на основі вчорашніх прогнозів, сьогодні виявляється неспроможною перед обличчям інформаційного вибуху, в результаті чого з’являється інформаційний стрес [8; 9].

Інформаційний стрес виникає зазвичай на підставі того, що психічні та фізіологічні можливості людини обмежені при сприйнятті інформації, і надалі може призвести до виникнення серйозних захворювань, пов’язаних з розладом нервової системи. Інформаційний стрес – це стан інформаційного перевантаження, коли суб’єкт (людина, суспільство) не справляється з поставленим завданням, не встигає приймати правильні рішення в необхідному темпі, будучи відповідальним за наслідки останніх [10]. Його викликають великі обсяги даних, які суб’єкт не в змозі осмислити і обробити, і високопродуктивні мережі. Навіть найсучасніші системи не справляються з покладеними на них завданнями, а найостанніша версія дорогого програмного забезпечення працює нестабільно. У цих умовах суб’єкт виявляється нездатним охопити всю інформацію, що надходить. Мало того, з цим завданням не справляється навіть програмне забезпечення.

Інформаційний стрес призводить до всіляких проблем психологічної інформаційної безпеки, ліквідувати його не вдається навіть шляхом встановлення нового обладнання.

Якби нові технології розвивалися по лінійній залежності, як кілька років тому, про інформаційний стрес можна було й не говорити: операційні системи встигали б обробляти всі масиви даних, пам’яті вистачало б для зберігання інформації, канали вводу/виводу не затримували б спільної роботи і т.п. Однак сьогодні цього не спостерігається. Виникає хвиля необроблених запитів і втрат продуктивності, і все разом це породжує інформаційний стрес [8].

Одна з функцій інформаційної культури – це захист від інформаційного стресу, який багато в чому породжується дисбалансом між зростаючим потоком інформації і здатністю суб’єкта (людини, суспільства) до її обробки [6; 7; 11].

У житті суб’єкта (людини, суспільства) неможливо знайти момент, коли останній не брав би участі в інформаційній взаємодії: виробництві інформації, її передачі та використанні. У процесі свого розвитку він, одночасно є споживачем, таким собі сховищем, “машиною” з обробки інформації та джерелом останньої. Інформація, яка поступає до суб’єкта, включається в надзвичайно складний і суперечливий процес формування установок по відношенню до тих чи інших цінностей. Інформація змінює у певному сенсі ті чи інші елементи свідомості людини та потім через неї – елементи суспільної свідомості. Поступово постійне виробництво і споживання інформації призводить до того, що її кількісне накопичення поступається місцем якісним змінам. Це, у свою чергу, призводить до виникнення проблем інформаційної безпеки суб’єкта (людини, суспільства), пов’язаних з негативним впливом інформації на її свідомість.

Інформаційна поведінка суб’єкта (людини, суспільства) у сучасному світі може носити активний і пасивний характер, це визначається рівнем його інформаційної культури. Забезпечення інформаційної безпеки суб’єкта, пов’язане з рівнем його інформаційної культури, причому, що вище цей рівень, то менше неприємностей виникає у людини з боку інформації і інформаційних технологій, що впливають на неї [12]. На цій підставі можна зробити наступний висновок: рівень інформаційної культури суб’єкта прямо пропорційний рівню інформаційної безпеки і, причому, що вище рівень інформаційної культури – то менше загроз останньої (тобто то вище рівень інформаційної безпеки).

На сучасному етапі розвитку інформаційного суспільства проблема забезпечення захисту суб’єкта-споживача інформації від шкідливого інформаційного впливу набуває особливого значення. Негативний момент полягає в тому, що позначена проблема тільки починає досліджуватися в нашій країні на теоретичному рівні, у зв’язку з цим, суттєвий інтерес представляє зарубіжний досвід у даній царині.

Один з найвидатніших теоретиків інформаційного суспільства – Елвін Тоффлер – у своїх роботах вперше описав негативні наслідки інформатизації і симптоми інформаційного стресу [13; 14]. Характеристикою інформаційного століття, за Е. Тоффлером, є зростання темпів виробництва й поширення інформації [13].

Високий темп інформатизації (або, в термінології Е. Тоффлера, надмірна стимуляція) вимагає від суб’єкта нового рівня адаптивності, який йому ще недоступний. Суб’єкт (людина, суспільство) не маючи необхідних стратегій виходу з цієї інформаційної кризи, схильний до хвороби, яку Е. Тоффлер називає “футурошок”, а ми називаємо інформаційним стресом. Дана хвороба представляє собою “людську реакцію на надмірну стимуляцію” [15, с. 37]. Він описує три рівні надмірної стимуляції, які впливають на поведінку суб’єкта:

- когнітивний рівень (на даному рівні розгляду відбувається надмірна стимуляція розумової діяльності суб’єкта, яка знижує його можливості у відборі, оцінюванні інформації, внаслідок чого, настає інформаційний стрес);

- рівень прийняття рішень (надмірні потоки інформації викликають у суб’єкта стрес, який заважає йому приймати будь-які рішення в той момент, коли це необхідно);
- сенсорний рівень (на цьому рівні здійснюється надмірна стимуляція почуттів суб’єкта, коли останній отримує велику кількість нової інформації, у нього знижується точність передачі образів, внаслідок чого пропадає бар’єр між реальним і віртуальним світами).

Е. Тоффлер також описує чотири стратегії поведінки суб’єкта, схильного до інформаційного стресу. Вони мають негативний відтінок, оскільки є результатом поганої адаптації суб’єкта до виникнення стресу [15, с. 38-39]:

- стратегія супер-спрощувача (суб’єкт намагається знайти одне спільне рішення для всіх проблем, що теж не дає бажаного результату);
- стратегія ревізіоніста (постійне повернення до стратегій, які в минулому змогли допомогти суб’єкту, але в даній ситуації вони не підходять);
- стратегія фахівця (полягає в ігноруванні суб’єктом усієї непотрібної інформації, крім розглянутого ним напрямку, однак така спеціалізація може застаріти під впливом невідомих зовнішніх і внутрішніх факторів);
- стратегія бар’єру (людина намагається виключити небажану реальність, вилучити весь потік нової інформації; суб’єкт, який використовує дану стратегію, намагається пристосуватися до змін, але все одно у нього будуть спостерігатися симптоми стресового стану).

Е. Тоффлер веде мову про те, що в даній ситуації необхідно виробити нові прийнятні стратегії для подальшого виживання суб’єкта (людини, суспільства). Однією з таких має бути розвиток інформаційної грамотності. Він пише: “Школа майбутнього повинна навчати не просто фактами, а тому, як класифікувати інформацію, як оцінити її правдоподібність, як спрогнозувати можливі негативні наслідки інформаційного впливу – як вчити себе” [15, с. 39].

У зв’язку з переліченими вище стратегіями Е. Тоффлер визначає багато з основних проблем інформаційного суспільства і, перш за все, проблему інформаційного стресу. Одним з перших він усвідомив, що розвиток інформаційної грамотності суб’єкта є стратегією виживання останнього в умовах інформаційних перевантажень.

Проблеми інформаційної грамотності суб’єкта в зарубіжній літературі часто розглядалися у взаємозв’язку з глибоким, вдумливим читанням. Найбільш повно ці питання розроблені у монографії С. Біркертса “Елегії Гуттенберга: Доля читання в електронному столітті” [16]. С. Біркертс висловлює ідею, яка полягає в тому, що пошуки правди (тобто того, що не можна поставити під сумнів; істини), яку намагається знайти суб’єкт (людина, суспільство) вимагають глибокого читання і глибокого мислення, тобто критичного мислення. Він говорить про те, що глибоке читання, або вертикальне читання, відноситься до періоду виникнення друкарства, коли наукової літератури майже не було: “Книга була чимось на зразок Біблії, яку постійно перечитували, а до деяких місць поверталися знову і знову для глибокого розуміння суті” [16, с. 62].

С. Біркертс протиставляє друковані та електронні тексти, відзначаючи, що лише перший є строго лінійним, ієрархічим і контрольованим, а в останньому: “Основний рух – горизонтально-асоціативний, а не вертикально-кумулятивний, як у друкованих текстах” [16, с. 54].

Він зазначає, що у візуальних засобах враження і образ переважає над логікою (тобто зоровий образ сприймається в основному ірраціонально, що й визначає нездатність суб’єкта до критичного оцінювання такої інформації). Ця втрата лінійності, ієрархічності і хронології за С. Біркертсом призводить до того, що вся інформація

сприймається як рівноцінна й доступна, це ускладнює її відбір і веде до інформаційних перевантажень. Такий стан він називає когнітивним колажем, який “впливає на увагу, здатність вчитуватися в текст, здатність розмірковувати над його складнощами, здатність витягти сенс з оригінального ритму й синтаксису”. Під глибоким читанням він розуміє “повільне, замислене оволодівання книгою” [16, с. 57], і робить висновок про те, що інформаційний простір є загрозою для критичного осмислення суб’єктом інформації, що веде до проблеми її диференціації.

Таким чином, подальша інформатизація суспільства і насичення його новими інформаційними технологіями ставить під загрозу саме існування вдумливого читання у сучасної людини.

Однією з центральних і часто обговорюваних проблем інформаційної безпеки є кількісний і якісний підходи до інформаційних перевантажень. Велика частина зарубіжних дослідників кінця XX століття займали сторону кількісного підходу (пов’язували інформаційні перевантаження з неймовірно великим обсягом інформації, в епіцентрі якого перебував суб’єкт-дослідник). Цієї позиції дотримувався й Е. Тоффлер, вважаючи, що постійно зростаючі обсяги нової інформації провокують футурошок. Однак він також писав про те, що, здобуваючи і структуруючи інформацію, можна розширити її жорсткі межі, після чого суб’єкт здатен критично її осмислити (він хотів сказати, що, підвищуючи якість інформації, можна до певної міри зняти кількісні обмеження) [15, с. 33].

Серед зарубіжних дослідників інформаційних перевантажень були також прихильники якісного підходу. Серед них: Б. Мільтон [17], Р. Оуен [18], М. Хілл [19] та інші. Вони вказували, що причиною інформаційного стресу є не надлишок інформації, а поява великих обсягів низькоякісної інформації, в результаті чого суб’єкт не міг її критично осмислити, тобто перетворити в знання. Б. Мільтон стверджував, що “Одна з іроній нового інформаційного століття полягає в тому, що перше, з чого завжди починається розмова про інформацію – те, що ми маємо її занадто багато...” [17, с. 8].

Інформації не може бути занадто багато, просто існує величезна кількість непотрібної інформації, яка змушує суб’єкта знати менше, аніж він знав до її отримання. Інформація – всього лише сировина, а рішення приймаються на основі знань, мудрості, інтуїції й розуміння, тобто продуктів її переробки [17].

Р. Оуен також виступає проти кількісного підходу. На його думку, неможливо провести чітку грань сприйняття інформації, оскільки суб’єкт має безліч ресурсів для їх обробки, кожен з яких має свої власні обмеження. Він усвідомлює, що ця межа, тобто гранична кількість інформації, яку суб’єкт може критично осмислити, залежить не від її кількості, а від майстерності обробки [18].

Сьогодні більшості зарубіжних дослідників стає зрозуміло, що причина інформаційного стресу пов’язана не з кількістю інформації, як ресурсу, а з її низькою якістю обробки [8].

Суть проблем, пов’язаних із забезпеченням інформаційної безпеки людини й суспільства, полягає в тому, що інформаційна сфера щодня розширюється дедалі більше і більше, як у обсязі, так і в сучасних засобах обробки інформації [20]. Таким чином, людина втрачає здатність контролювати те, що відбувається, що призводить до зростання її внутрішньої напруженості й виникнення стресових ситуацій [21, с. 81].

Висновки.

Інформаційна безпека – одна з гострих соціокультурних проблем сучасного суспільства, яка має системний характер і торкається діяльності основних інститутів і підсистем; у контекст її впливу потрапляють ключові соціокультурні процеси, що

відбуваються в суспільстві. Ключовим фактором ризику для інформаційної підсистеми соціуму виступають масштабні соціокомунікативні та соціокультурні трансформації, що несуть у собі низку негативних соціальних наслідків. В останні роки чітко фіксуються дезорганізаційно-дисфункційні тенденції, безпосередньо пов’язані з високими швидкостями інформаційних змін.

Надлишок низькоякісної інформації, який спостерігається на даному етапі розвитку інформаційного суспільства є не єдиною проблемою забезпечення інформаційної безпеки. У дану проблематику також входить проблема формування у людини відповідного рівня інформаційної культури, який перешкоджав би виникненню у неї стресових ситуацій при роботі з інформацією та інформаційними технологіями.

Формування у сучасного суб’єкта відповідних навичок і умінь для роботи в інформаційній сфері – це завдання не тільки системи освіти, про що сьогодні ведуть мову найчастіше, а й кожного індивіда окремо. Тому забезпечення інформаційної безпеки у сучасному суспільстві залежить від багатьох факторів, у тому числі й від того, як буде поводитися людина в тій чи іншій стресовій ситуації.

Використана література

1. Кастельс М. Информационная эпоха : экономика, общество и культура / М. Кастельс ; [пер. с англ. под науч. ред. О.И. Шкаратана]. – М. : Гос. ун-т. Высш. шк. экономики, 2000. – 606 с.

2. Дзьобань О.П. Філософія інформаційних комунікацій : монографія / О.П. Дзьобань. – Харків : Майдан, 2012. – 224 с.

3. Дзьобань О.П. Інформаційне насильство та безпека : світоглядно-правові аспекти : монографія / О.П. Дзьобань, В.Г. Пилипчук ; за заг. ред. проф. В.Г. Пилипчука. – Харків : Майдан, 2011. – 244 с.

4. Дзьобань О.П. Інформаційна безпека у проблемному полі соціокультурної реальності : монографія / О.П. Дзьобань. – Х. : Майдан, 2010. – 260 с.

5. Маркозова О.О. Досягнення життєвого успіху людини в умовах інформаційного перевантаження // Вісник Національного університету “Юридична академія України імені Ярослава Мудрого” ; редкол. : А.П. Гетьман та ін. – Х. : Право, 2016. – № 4 (31). – С. 175-182. – (Серія : Філософія).

6. Прудникова О.В. Інформаційна культура : концептуальні засади та світоглядний сенс : монографія / О.В. Прудникова. – Х. : Право, 2015. – 352 с.

7. Прудникова О.В. Інформаційна культура в інформаційному суспільстві // Науковий часопис Національного педагогічного університету імені М.П. Драгоманова. : зб. наукових праць ; за заг. ред. В.П. Андрущенка. – К., 2013. – Вип. 30 (43). – С. 159-166. – (Серія 7. Релігієзнавство. Культурологія. Філософія).

8. Калиновская Н.А. Информационный стресс. Информационно-психологическая безопасность личности как качественная характеристика информационной культуры человека : монография / Н.А. Калиновская, Д.Ю. Устимов. – Режим доступа : http://www.twirpx.com/file/354820

9. Терещенко Э.В., Есаян М.Л. Информационный стресс: психологические и социальные аспекты. – Режим доступа : http://www.rusnauka.com/6_PNI_2012/Psiholog ia/12_102600.doc.htm

10. Дзьобань О.П., Мануйлов Є.М. Сучасне суспільство як суспільство з деформованою відповідальністю (за працею З. Баумана “Індивідуалізоване суспільство”) // Вісник Національного університету “Юридична академія України імені Ярослава Мудрого” ; редкол. : А.П. Гетьман та ін. – Х. : Право, 2016. – № 4 (31). – С. 14-26. – (Серія : Філософія).

11. Прудникова О.В. Антропологічні обрії інформаційної культури віртуального простору // Політологічний вісник : зб. наукових праць. – К., 2014. – Вип. 75. – С. 71-80.

12. Чурашева О.Л. Информационная культура и информационная безопасность личности // Теория и практика общественного развития. – 2014. – № 16. – С. 188-190.

13. Тоффлер Э. Футурошок / Элвин Тоффлер. – СПб. : Лань, 1997. – 461 с.

14. Тоффлер Э. Шок будущего / Элвин Тоффлер ; [пер. с англ.]. – М. : Издательство АСТ, 2001. – 557 с.

15. Toffler A. The Third Wave / A. Toffler. – Toronto (etc.) : Bantam Books, 1981. – 394 p.

16. Birkerts S. The Gutenberg Elegies: The Fate of Reading in an Electronic Age / S. Birkerts. – Режим доступу : http://archives.obs.com/obc/english/books/nn bdbirk.html.

17. Milton B.G. Making Sense or Non-sense : Key Issues in the Information Age // Canadian Vocational Journal. – 1989. – Vol. 24. – № 3. – P. 5-9.

18. Owen R.S. Clarifying the Simple Assumption of the Information Load Paradigm. – Режим доступу : http://www.acrwebsite.org/search/view-conference-proceedings.aspx?Id=7387/.

19. Hill M.W. The Impact of Information on Society : An Examination of it's Nature Value and Usage / M.W. Hill. – London : Bawker, 1999. – 292 p.

20. Дзьобань О.П., Мануйлов Є.М. Соціокультурні аспекти інформаційної безпеки : матеріали IX Симпозіуму [“Соціально-економічний розвиток системи фінансів і управління в інноваційному середовищі : проблеми, ефективність, перспективи”], (Харків, 25 листопада 2016 р.) / Міністерство освіти і науки України ; Харківський інститут фінансів Київського національного торговельно-економічного університету. – Харків : РВВ ХІФ КНТЕУ, 2016. – С. 368-369.

21. Боковиков А.М. Модус контроля как фактор стрессоустойчивости при компьютеризации профессиональной деятельности // Психологический журнал. – 2000. – № 21. – С. 93-101.

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

УДК 34(3/9)+930.85

ВРОНСЬКА Т.В., *доктор історичних наук, старший науковий співробітник,*
головний науковий співробітник
НДІ інформатики і права НАПрН України
БЕЛАНЮК М.В., *кандидат юридичних наук,* завідувач наукового організаційного сектору
НДІ інформатики і права НАПрН України

ДАВНЬОІНДІЙСЬКИЙ ТРАКТАТ “АРТХАШАСТРА”[1] В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОТИДІЇ НЕГАТИВНИМ ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИМ ВПЛИВАМ

Анотація. *У статті крізь призму забезпечення інформаційної безпеки та протидії сучасним інформаційним операціям проаналізовано історичну давньоіндійську пам’ятку – трактат “Артхашастра”, укладену понад два тисячоліття тому, яка й нині має важливе прикладне значення, оскільки у ній висвітлені глибинні рушійні сили застосування деструктивного інформаційного впливу на різні групи громадян та широкий арсенал його методів.*

Ключові слова: *оперативно-розшукова діяльність, інформаційно-психологічні операції, оперативні ігри, комбінації, легендування, маніпуляція, провокація, дискредитація, компрометація, дестабілізація, дезорганізація.*

Аннотация. *В статье сквозь призму обеспечения информационной безопасности и противодействия современным информационным операциям проанализирован исторический древнеиндийский трактат “Артхашастра”, созданный более двух тысячелетий назад, который сейчас имеет важное прикладное значение, поскольку в нем освещены глубинные движущие силы применения деструктивного информационного воздействия на различные группы граждан и широкий арсенал его методов.*

Ключевые слова: *оперативно-розыскная деятельность, информационно-психологические операции, оперативные игры, комбинации, легендирование, манипуляция, провокация, дискредитация, компрометация, дестабилизация, дезорганизация.*

Summary. *The article in the light of information security and counteraction to modern information operations analyzes the ancient Indian historical treatise “Arthashastra”, which was composed more than two millennia ago and still has important practical significance, since it highlights the underlying drivers of the use of destructive information impact on different groups of citizens and wide arsenal of its methods.*

Keywords: *detective and search activities, information and psychological operations, operation games, combinations, legendizing, manipulation, provocation, defamation, compromise, destabilization, disorganization.*

Постановка проблеми. Проблематика забезпечення інформаційної безпеки та протидії інформаційно-психологічним операціям, зокрема і в контексті діяльності правоохоронних органів та спецслужб, настільки багатогранна і складна, що й донині залишається недостатньо розробленою. Це стосується не лише історичного досвіду, а й

[1] “Артхашастра” (“Наука політики”, “Наука про державний устрій”) – політико-економічний трактат давньої Індії, датований орієнтовно IV-III ст. д.н.е. – I ст. н.е., авторство якого приписується брахману Каутільї. Російською мовою твір було перекладено у 1932 р. групою вчених Інституту сходознавства АН СРСР. Доопрацьований переклад вийшов друком у 1959 р. під назвою “Артхашастра или наука политики”. Перевод с санскрита. Издание подготовил В.И. Кальянов. Издательство Академии наук СССР. – Москва-Ленинград, 1959. – 798 с.

теоретичних надбань цієї галузі, зокрема й тих, що сягають своїм корінням у товщу минулих тисячоліть.

Сьогодні важко навіть уявити, як за відсутності засобів масової комунікації методологія інформаційно-психологічного впливу, ретельно приховувана маніпуляторами (ініціаторами та виконавцями), передавалася крізь століття. Як би там не було, але ці знання, класифіковані та узагальнені (навіть у супроводі теоретико-методологічних порад з їх використання у дипломатичній, військовій, розвідувальній та правоохоронній діяльності), дійшли до нас у концентрованому (практично незмінному вигляді). Найбільш відомим з них є “Трактат про військове мистецтво” (датований приблизно V ст. до н.е.) в авторстві китайського полководця, воєнного теоретика і філософа Сунь-Цзи. Є й низка інших джерел, завдяки яким хоча б фрагментарно видається можливим простежити еволюцію елементів інформаційно-психологічних операцій у розвідувальній та правоохоронній діяльності [1, с. 115-200]. Значно менший дослідницький інтерес у згаданому контексті простежується до іншого пам’ятника великої історичної цінності – давньоіндійського трактату “Артхашастра”.

Методологічною основою роздумів автора трактату є впевненість в незмінності науки управління державою та незмінності природи діяльності людини та мотивів її поведінки.

Лінійне (спрощене) сприйняття “Артхашастри”, як праці, начебто застарілої і несучасної, є помилковим, з огляду на детальні рекомендації використання таємних агентів (шпигунів) і сфер їх діяльності. Вони суголосні (хоча й відмінні у лексичних формах) і багато в чому збігаються за змістом з багатьма “профільними” документами радянських спецслужб і теоретичними напрацюваннями відповідного профілю ХХ ст. Окрім суто прикладного характеру їх використання, аналіз витоків цільових інформаційно-психологічних маніпулятивних впливів на особу чи певні соціальні групи диктується й необхідністю формування ефективної системи ефективного соціально-психологічного захисту, створення певного імунітету.

Мета статті. Не претендуючи на вичерпність, пропонуємо здійснити теоретико-історичний екскурс у товщу минулих тисячоліть, ознайомитися з концептуальними поглядами автора давньоіндійського трактату “Артхашастра”, порівнявши його концептуальні положення та пропоновані методи інформаційно-психологічного впливу на різні верстви населення з відповідними теоретичними засадами діяльності радянських надзвичайних органів.

Виклад основного матеріалу. Компрометація, дискредитація, маніпуляція, розклад, дезінформація відомі людству з найдавніших часів. Ці дії ставали знаряддям прихованого або обманного характеру, що здійснювалися з метою здійснення завдань внутрішньої та зовнішньої політики держави. Це універсальний інструмент всіх часів і народів, що призводив до знищення армій, руйнування держав, тріумфу окремих народів та особистостей або краху тисячолітніх імперій. Трактат “Артхашастра” – праця, що не лише ілюструє політичний зріз своєї епохи, а й доводить, що інформаційно-психологічні операції широко застосовувались у політичній, економічній і соціальній сферах життя держави, суспільства і людини. Те, навіть доволі обмежене коло дослідників, які аналізували давньоіндійський трактат “Артхашастра” у контексті вивчення різних аспектів дипломатичної та військової сфери, чомусь обходили теоретичні засади правоохоронної та контррозвідувальної діяльності, не висвітлювали інші його аспекти, пов’язані з цільовими психологічними впливами на певні групи громадян. Вітчизняний політолог Дмитро Видрін, який працював з цією працею у київській історичній бібліотеці у другій половині 80-х років ХХ ст., стверджував, що

“Артхашастру” *“з моменту її видання російською мовою, ще на початку 30-х років ніхто [з книгосховища] жодного разу не брав і тим більше не цитував”*. Він, подаючи переклад назви трактату як *“наука про господарювання, правда про владу”*, характеризує це джерело як видатне і аналізує його у контексті свого основного фаху, назвав цю працю *“Біблією або катехізисом політичних знань…, точним і детальним описом всіх мислимих і немислимих політичних проблем й способів їх вирішення”* [2]. Інший дослідник Д. Заяць пізніше звертався до цієї ж праці у загальному контексті вивчення проблем державного управління та зауважував, що “Архашастра” є прикладом *“індійської парадигми менеджменту*” [3, с. 204-208]. Вітчизняний дипломат Р. Пиріг аналізував положення трактату крізь призму своєї професійної діяльності [4]. Інші науковці – спеціалісти з комунікативних технологій, філософії, політології, військового мистецтва, тощо, згадували цю працю лише побіжно – у контексті загального огляду історичної спадщини [5].

Тим часом поза увагою залишилася дуже важлива змістовна складова цього давньоіндійського трактату, яка дозволяє не лише поглибити сучасні уявлення про історичні витоки теорії та практики інформаційно-психологічних операцій, а й розширити знання про практику їх застосування у давні часи.

Більшість структурних підрозділів трактату вже своїми – доволі промовистими назвами (“Випробовування чесності та нечесності міністрів хитрощами”, “Призначення таємних агентів”, “Дії, що викликають розбрат в [політичних] об’єднаннях [всередині держави та за її межами]”, “Війна за допомогою інтриг”, “Про шпигунів [диверсантів], що діють зброєю, вогнем, отрутою”, “Підбурювання та наклепи у середовищі ворогів”, “Про застосування таємних агентів”, “Застосування засобів обману”) тощо вказують на широке поле таємної діяльності. Очевидно й те, що навіть за відсутності відповідних організаційних (державних) структур у ті часи здійснювалася правоохоронна та контррозвідувальна діяльність з використанням відповідних методів, які є складовими інформаційно-психологічних операцій. У праці містяться унікальні теоретичні положення та практичні поради, які придатні й сьогодні, зокрема й у плануванні та реалізації оперативних ігор з використанням методу легендування. Щоправда, автор праці оперує термінами “агенти” та “шпигуни”, іноді й синонімічно, що не завжди відповідає сфері їх діяльності всередині держави та за її межами.

Звертає на себе увагу і та обставина, що розвідувальна діяльність перебувала як в одноосібній компетенції послів, так і керівника держави та окремих вищих сановників. В одному з абзаців розділу 144 “Особи пов’язані з внутрішніми ворогами та зовнішніми” у досить своєрідний спосіб декларовані ієрархія, компетенція та сфера відповідальності у таємній роботі держави: *“Успіх головного агента залежить від царя; успіх зусиль, що прикладаються, залежить від головного радника; успіх, отриманий від головного агента, залежить від обох (від царя та радника)”* [6, с. 402].

У трактаті окремо виписані рекомендації для розвідників, підпорядкованих винятково послу, який також мав видобувати інформацію про різні сфери життєдіяльності країни перебування. *“Здійснюючи свою місію в іншій державі, посол повинен збирати інформацію, спілкуючись із її чиновниками, вивчати місця розташування військ, міцність укріплень, фінансовий стан держави, її продовольчу безпеку, стан охорони чутливих об’єктів”* [6, с. 39], – декларувалося в “Артхашастрі”. Дипломат високого рангу, окрім іншого, повинен підтримувати ворожі до місцевої влади політичні об’єднання та групи, сприяти підбурюванню суперечок між союзниками країни перебування (розриванню договорів), таємному перекиданню військ, викраденню родичів і коштовностей (ворога), отриманню інформації від шпигунів;

налагоджувати роботу шпигунів, які вивчають внутрішньополітичну ситуацію, її слабкі місця, а також отримувати відповідну інформацію через моніторинг настроїв найнижчих верств населення [6, с. 40, 437].

Подібні завдання з метою заподіяння шкоди у сфері зовнішньої політики, а також ускладнення міжнародних стосунків формулювалися і в перші роки існування радянської влади в одному з регламентних документів з організації агентурної розвідки за кордоном. Резиденту доручалося поширювати чутки, які можуть посіяти ворожнечу між цією державою та її союзниками; створювати між ними тертя шляхом викриття таємних договорів, організація і усіляке сприяння економічним заворушенням, страйкам, обструкціям тощо [7, с. 24].

У контексті викладеного в “Артхашастрі” напрочуд суголосними видаються пропозиції радянського чекіста С. Турло, викладені ним ще на початку 20-х років ХХ ст. Він вбачав завданням активної розвідки за кордоном у *“…сприянні зростанню загального невдоволення [місцевого населення]; компрометацію членів уряду або насильницьке їх усунення; провокацію громадянських заворушень і безладу; розпалювання політичної та національної ворожнечі; дезорганізація урядової партії та її дискредитація в очах населення”* [8, с. 22]. Згаданий співробітник радянських спецслужб, як, власне, і автор “Артхашастри”, вважав, що *“Вона* (активна дипломатична розвідка – *Авт.) не знає ніяких законів, в т.ч. і моральних, і виношуючи свою мету, пускає в хід усі засоби без вибору, якщо тільки застосування їх для неї вигідно і корисно”* [8, с. 22].

З іншого боку, у “Артхашастрі” викладені рекомендації щодо налагодження контррозвідувальних заходів, сфокусованих на “акредитованих” іноземних послів у власній державі. Не менш детально виписана аналогічна діяльність у прикордонній смузі, з виразним наголосом на необхідності правил суворої конспірації особливо досвідченими і перевіреними особами (“головними шпигунами”) [6, с. 40].

З метою ретельного контролю професійно-моральних якостей своїх власних чиновників вищого рангу, у трактаті пропонувався певний алгоритм перевірки їх відданості владі. У першій частині праці (розділ 10) “Випробовування чесності і нечесності міністрів хитрощами” пропонуються певні сценарії перевірки вищих посадовців, зокрема і шляхом створення ситуації, коли одного з них (міністра) ув’язнюють [начебто, за підозрою у скоєнні якогось злочину] і вже під час перебування у камері через підсадну особу (“шпигуна під виглядом учня, вміщеного туди заздалегідь”) провокують до відвертих розмов, аби виявити “чистоту” його намірів [6, с. 26]. Отже внутрішньокамерна розробка затриманих (арештованих), як метод оперативно-розшукової діяльності, детально виписаний в “Архашастрі”.

Взагалі збиранню, накопиченню та конструктивному використанню інформації автор трактату приділяє дуже серйозну увагу. Ефективне протиборство, на його переконання, досяжне лише після отримання всебічних знань про можливості (потенціал) противника, його слабкі та сильні сторони (якості). А сформувати таку обізнаність можливо лише узагальнивши всю інформацію, отриману шляхом розвідувальної діяльності.

Згадуваних у тексті “Артхашастри” агентів, шпигунів (розділ 7, глава 11 “Створення групи шпигунів”) [6, с. 27-29] пропонувалося підбирати різноманітними способами, зокрема й серед осіб, які через низку обставин зазнали фіаско за своїм основним фахом (родом діяльності) і тому можуть легко впроваджуватися (адаптуватися) у звичне (знайоме) середовище, де треба здобувати інформацію [6, с. 27-28].

У розділі “Використання таємних агентів” детально викладається процедура легалізації згаданих осіб у певних соціальних колах як всередині держави, так і за її

межами. Ретельно аналізуються особисті якості людей, яким за наказом треба буде займатися спостереженням, вчиненням терактів й фізичним усуненням певних осіб. Приміром для “найманців-убивць”, на переконання автора “Архашастри”, придатні хоробрі особи, які стимульовані матеріальною винагородою. *“Позбавлені любові до близьких, жорстокі та з мінливим настроєм – це отруйники”*, – наголошував автор трактату [6, с. 29].

Узагальнивши сфери застосовування “агентів” і “шпигунів”, виписані в “Артхашастрі”, користуючись сучасною термінологією та історичними реаліями їх діяльності у різні періоди, зокрема і в підрозділах радянських спецслужб, видається можливим стратифікувати цих фахівців таким чином:

а) особи, підпорядковані вищій владі, які здійснювали суто розвідувальну діяльність за межами держави, не виконуючи інших функцій; б) розвідники-диверсанти, призначені для застосування активних методів на території супротивника; здійснення терористичних актів на стратегічних об’єктах і залюднених місцях, фізичного усунення лідерів, зокрема політиків та воєначальників, та осіб, які охороняють важливі об’єкти та ін.; в) агенти-дезінформатори, завданням яких є сіяння неправдивих чуток і панічних настроїв у певних колах як всередині власної держави, так і за її межами; г) таємна агентура – провокатори, впроваджені у середовище противника з метою компрометації певних осіб (для підкидання зброї, вибухівки), наперед знаючи, що все це буде виявлене і потягне за собою відповідні дії влади; розповсюдження свідомо викривленої інформації, спрямованої на створення конфліктних ситуацій, сіяння розбрату, ворожнечі, підбурювання до неправомірних дій; в) подвійні агенти – “шпигуни, які отримують матеріальну винагороду від обох сторін” та інші, які працювали одночасно в інтересах кількох держав.

У трактаті пропонуються і способи перевірки отриманих розвідувальних даних шляхом їх аналітичного опрацювання: *“Якщо покази трьох шпигунів збігатимуться, то їм довіряти”*. Коли ж виникатимуть підозри щодо сфальшованої або недостовірної інформації у “Артхашастрі” рекомендується таке: *“У випадку кількох (повторюваних) розбіжностей показів [розвідувальної інформації] застосовується покарання або усунення шпигуна”*, який подав неправдиві дані [6, с. 30].

Серед іншого в “Архашастрі” знаходимо й пропозиції по одночасному впровадженню у вороже середовище двох агентів з різними легендами, які, не знаючи один одного, повинні досягти поставленої мети [6, с. 29]. Така “підстраховка” мала сприяти успіху операції. У цьому ж контексті слід згадати настанови трактату щодо створення легенд для кожного з розвідників (агентів), які мали безперешкодно та правдоподібно легалізуватися у ворожому середовищі.

До речі, так само діяли і радянські спецслужби, коли у першій половині 30-х років XX ст., плануючи вбивство Є. Коновальця, під різними легендами просували у його найближче оточення радянських агентів: К. Полуведька під виглядом утікача з Соловецького табору (1934 р.) та П. Судоплатова, який, начебто, перетнув кордон СРСР у пошуках спільників у боротьбі з тоталітарним режимом [9, с. 19-36].

Комплекс дій, які становили те, що нині йменується інформаційно-психологічними операціями, оперативними іграми, зокрема і ті, які мали на меті встановлення контролю за опозицією, її нейтралізацію всередині держави, позбавлення підтримки ззовні, знешкодження очільників, здатних до повалення існуючого режиму тощо, представлені у більшості структурних підрозділів “Артхашастри”.

Так, у першій частині трактату “Спостереження у власній державі за партіями людей відданих і налаштованих на зраду” (розділ 9), “Залучення [на свій бік] осіб з

партій іншої держави, схильних до зради” (розділ 10) [6, с. 24-27] та у наступних, зокрема, “Дії, що викликають розбрат (в об’єднаннях)” (розділ 160), “Таємні вбивства” (розділ 161) [6, с. 431-434] детально викладаються сценарії послідовних дій (провокація, залякування, сімейне заручництво, компрометація, сіяння неправдивих чуток, відволікання уваги й перефокусування на менш значущі речі тощо) задля досягнення кінцевої мети.

Автор “Артхашастри” радить уважно вивчати психогенні характеристики об’єктів впливу (або вербування) задля успішного використання тієї чи іншої особи на свою користь, наголошуючи, що особливу увагу слід звертати на такі риси: *“пристрасність, гнів, нерішучість, м’якість, сором’язливість, гордість, жалість, обман, жадібність, заздрість, зневага до свого оточення, злостивість, недовіра, страх”* [6, с. 399].

Передусім, виокремлюються вразливі для психологічного впливу категорії: родичі несправедливо репресованих й переслідуваних; дискриміновані за різних обставин, позбавлені майна та спадщини, зневажені, звільнені з роботи. Іншими словами – ображені на владу. Виділяли й тих, хто дійсно вчинив неправомірні дії і був покараний за це, зазіхав на майно царя або його близьких; жадібних, скупих, порочних, пихатих тощо. Всі ці категорії “ображених” і “схиблених” трактат радив шляхом підкупу залучати до співпраці в опонентських угрупованнях і за межами держави. Тих, хто не йшов на це, приписувалося привертати на свій бік іншими – підступними методами (інтригами, залякуванням тощо) [6, с. 35].

Фокусуючи свою увагу на зовнішніх ворогах – у сусідніх державах, автор давньоіндійського трактату, вірогідно, як прибічник авторитарної форми правління, волів “стабільності” за будь-яку ціну, зокрема і шляхом повної покори власного населення. Так, серед іншого наголошувалося, що “*заворушення (хвилювання) всередині [держави] більш небезпечні, ніж ті, що відбуваються ззовні (за її межами)”.* Слушним у контексті такої політики видається й інше твердження: *“Коли зовнішні [вороги] перебувають у змові з внутрішніми і [навпаки] внутрішні із зовнішніми, то в обох випадках змовники мають шанс на успіх”* (розділи 143, 144). Не обмежуючись констатацією, автор трактату радить вдаватися до відповідних кроків: *“Примиренням треба досягати мети з тими, у кого виснажені сили, хто втомився від боротьби, чиї засоби вичерпані, хто змучений втратами людей та майна й вигнанням, хто бажає отримати (нового) друга через благородство, хто сумнівається в іншому, хто ставить на перше місце дружбу, хто чесний… Подарунками треба досягати мети з тим, хто жадібний і слабкий…”* [6, с. 403].

Розділи “Війна за допомогою інтриг”, “Про вбивство воєначальників. Сіяння розбрату у колі держав”, “Знищення (ворога) шляхом таємних заходів…”, вміщені у XII відділі “Артхашастри”, вже самі назви вказують на зміст і методи. Так, у першому з перелічених розділів досить докладно описується, як можна залякати незговірливого противника, а також уникнути можливих негативних наслідків у разі непоступливості об’єкта впливу [6, с. 438-449].

Психологічні операції, метою яких є деморалізація цивільного населення в країні противника або на загарбаній ним території, також описуються досить детально. Агентам впливу на окупованій території пропонується поширювати чутки серед місцевого населення про те, що керівники, начебто, свідомо залишили їх напризволяще, спричиняючи у такий спосіб гнів та наступні кроки ображених і зраджених аж до фізичного усунення учорашніх лідерів. Інші інсинуації, спрямовані на розповсюдження неправдивої інформації стосовно мародерства та інших злочинів з боку провідників: *“*(*Таємні агенти) повинні спалювати внутрішні хороми, міські ворота і зерносховища і*

вбивати людей, які їх охороняють. Потім із сумним виглядом вони повинні оголосити, що (підпали) здійснені ними (тобто вбитими)” [6, с. 438-441].

Серед рецептів руйнування опору у фортецях противника “Артхашастра” радить також використовувати провокації, поширення чуток, зокрема і про те, що керівники залишили напризволяще тих, хто чинить запеклий спротив [6, с. 430-431].

Не менш ретельно, ніж інші методи роботи, для шпигунів прописано й інше “поле діяльності” (розділи 166-170) “Про шпигунів, які діють зброєю, вогнем, отрутою...”, “Знищення ворога таємними засобами…”). Власне, йдеться про диверсійно-терористичну діяльність. Рекомендується руйнація стін храмів під час перебування там державного діяча, “прогнозоване” падіння каміння, застосування отрути, знищення припасів їжі та води, заманювання до пасток, зокрема і шляхом підведення неправдивої інформації, реагуючи на яку збройні сили, чи сановник високого рангу опинявся перед загрозою загибелі [6, с. 444-448].

Розділи “Артхашастри”, присвячені підготовці до війни і веденню бойових дій, містять чимало прикладів організації інтриг і створення “п’ятої” колони в тилу ворога, тобто багато такого, що й дотепер використовується творцями психологічних операцій.

Усі поради супроводжуються конкретними прикладами і можливими сценаріями у разі непередбачуваного розвитку подій. Наводиться безліч способів фізичного усунення противника (виготовлення отрути з рослин, комах та дрібних тварин), як і способів уникнення наглої смерті.

Не менш цікавими видаються і ті положення трактату, які повчають як саме треба діяти, аби розколоти політичні угруповання, які становлять небезпеку для верховної влади. Вже сама назва розділів 160 та 161 “Дії, що спричиняють чвари (в об’єднаннях) та таємне вбивство” є доволі промовистою та не вимагає додаткових коментарів. Там містяться рекомендації, як агенти мають просочуватися до цих груп, фіксувати вразливі якості їх членів, підігрівати взаємні розбіжності, ворожнечу і сварки, підбурювати до непокори керівнику. Окрім цього вони мають спрямовувати свої зусилля на підрив авторитету керівника цього політичного об’єднання, створюючи штучні перепони для їх ефективної діяльності. У трактаті про це написано наступним чином: *“…вони повинні сприяти чварам наступним чином, ведучи мову, приміром у такому напрямі: “Ось такий-то обмовляє тебе”. Такі підбурювання треба робити стосовно обох сторін (які бажано посварити)”. Коли між членами об’єднання буде посіяна ворожнеча, то шпигуни, під виглядом вчителів, повинні створити привід до інших – дрібніших сварок…”* [6, с. 430-431].

Але й зазначені методи не вичерпують всього арсеналу, рекомендованого “Артхашастрою”, зокрема і для виявлення та нейтралізації політичних угруповань всередині держави. Як і на інших ділянках боротьби з опонентами та противниками, тут головну роль мали відігравати таємні агенти, які мали реалізовувати добре інсценовані провокації. *“Государ має для видимості вигнати відданого йому главу об’єднання. Останній робить вигляд, що шукає захисту у ворога того, хто його вигнав”*, – радить автор трактату. Продовжуючи, він наголошує, що “вигнанець” під приводом вербування симпатиків, прибічників (начебто, для організації спротиву та боротьби) повинен підшукати спільників. Далі, маючи достатню підтримку з боку таємних агентів, він сприяє фізичному усуненню цих дезінформованих “зрадників” [6, с. 460]. Окрім цього, пропонувалося знайти джерело повідомлення про начебто існуючу “ворожо налаштовану партію” для усунення її прибічників як всередині держави, так і за її межами. Іншими словами, реалізовувалися фіктивно-провокаційні комбінації (оперативні ігри), до яких вдавалися у 20-30-ті роки ОДПУ-НКВС, ліквідовуючи своїх

реальних і потенційних політичних опонентів. В одному з документів ДПУ УСРР від 2 березня 1926 р. (“Орієнтування по активній українській контрреволюції”) підкреслювалося, що черговим завданням є виявлення симпатиків української еміграції в Україні та стовідсоткове охоплення її агентурою. У документах радянських спецслужб тих часів ця робота висвітлювалась під промовистою і недвозначною назвою “Фіктивно-провокативні організації ДПУ по українській лінії” [9, с. 21]. Серед агентурних матеріалів “білої” контррозвідки, датованих 1927 р., є цікаві документи, що за своїм змістом схожі на положення, викладені у давньоіндійському трактаті. Зокрема, йдеться про записку під назвою “Деякі міркування з приводу боротьби ДПУ з контрреволюційними організаціями” [10, с. 1-2], де досить розлого викладені всі методи боротьби з опонентами радянської влади за кордоном. Автор записки[2] формулює мету і завдання радянських органів держбезпеки: засобами агентурної роботи створити фіктивну “контрреволюційну” організацію за кордоном і керувати нею, втягуючи у свої тенета якомога більше членів на теренах СРСР.

Повертаючись до аналізу давньоіндійського трактату, слід зазначити, що його автор неодноразово концентрував свою увагу на необхідності вивчення слабких сторін голів певних політичних угруповань та осіб амбітних, які конкурували між собою, зазіхаючи на місця у верхівці, автор трактату радить: *“Слід розділяти тих, хто ненавидить один одного, ворогують між собою, побоюючись захоплення землі один у одного”*. Користуючись сучасною мовою, можна екстраполювати це на складові боротьби олігархів за сфери впливу. Далі він рекомендує підмовляти конкурентів, підкидаючи неправдиву інформацію щодо укладання таємних союзів поза спиною; апелювати до, начебто, прихованого навіть від союзників ведення вигідного бізнесу з зовнішнім ворогом: *“Якщо з своєї держави або чужої ідуть товари на сховища ворога, то агенти повинні направлятися, аби спровокувати конфлікт, повідомити одному з конкурентів: “вони [товари] отримані від того, хто уклав таємний союз з отримувачем”* [6, с. 403].

В “Артхашастрі” містяться також й інші поради, спрямовані на розривання певних союзів шляхом розповсюдження неправдивих чуток, сіяння розколу та чвар. Особливу роль у цій справі мають відігравати подвійні агенти.

Компрометація вищого керівництва держав противника, розповсюдження про нього сфальшованої інформації, підбурювання на виступи проти влади – все це детально описане у розділі 164-165 “Про сіяння смути”, яке перебувало у компетенції агентів, які легалізувалися в інших державах під виглядом місцевих мешканців. Цим особам для знищення авторитету та повалення державного діяча трактат, окрім іншого, дає настанови провокувати жадібність родичів, а також тих, кого дискримінують [6, с. 443].

---

[2] Автором записки, як уже встановлено, був Володимир Орлов (1882-1941 рр.) – дійсний статський радник, слідчий в особливо важливих справах при штабі Західного фронту в період Першої світової війни, видатний російський контррозвідник. Нелегально працював у ВЧК (комісія у кримінальних справах) у 1917-1918 рр., куди він проник за завданням генерала М. Алексєєва. У 1918 р. був викритий більшовиками і змушений за допомогою німців утекти з Одеси. Згодом перебрався до Берліна. Створив архів, де зберігалися досьє на багатьох діячів радянської держави, партійних функціонерів, дипломатів, розвідників системи Іноземного відділу (ІНВ) ОДПУ-НКВС. Укомплектував пакет регламентних документів для практичної діяльності денікінської контррозвідки. До згаданого пакета потрапили і ті документи, які він “прихопив” із собою з ЧК, де певний час нелегально працював. Загинув при загадкових обставинах у 1941 р. Є припущення, що його вбили гітлерівці, проти яких він виступав так само рішуче, як і проти більшовиків.

Слід підкреслити, що метод компрометації доволі активно використовувався і радянськими спецслужбами. Так, в Інструкції, виданій ОДПУ у 20-х рр. ХХ ст. для агентів за кордоном, чітко виписувалися схожі на ті, що містяться в “Артхашастрі”, методи впровадження розколу ворожої організації, підмінювання ідей; дискредитації провідників антирадянських політичних партій перед їх власними однодумцями, зокрема і шляхом очорнення особистого життя, поширення інсинуацій щодо чистоти їх намірів, надмірних амбіцій тощо [11, с. 216].

Аналізуючи все розмаїття методів виявлення опозиційно налаштованих окремих осіб та угруповань всередині держави, автор “Артхашастри” радив монарху вживати запобіжних заходів від деструктивних впливів громадян своєї держави: *“Мудрий цар у своїй державі нехай охороняє відданих людей від впливів й підбурювань ворогів”* [6, с. 33].

Поради і рекомендації автора “Артхашастри” на двадцять чотири століття пережили свого автора і сьогодні застосовуються не лише в інформаційно-психологічних операціях спецслужб і дипломатичних відомств проти зовнішнього ворога, а й у внутрішньополітичному житті. Зокрема, у трактаті зазначено: *“Залучення на свій бік об’єднання (групи людей, політичної партії противника і всередині власної країни) є більш істотним, ніж придбання військ або союзників. Справді, завдяки своїй згуртованості об’єднання нездоланні для інших. Якщо такі об’єднання прихильні (до заінтересованого правителя), то останній повинен їх використовувати (залучаючи їх до себе) люб’язностями та подарунками. Об’єднання ж, налаштовані вороже, треба долати, сіючи серед них розбрат, і відкритою силою…”* [6, с. 449].

Даються конкретні поради стосовно методів впливу на окремі категорії осіб для досягнення кінцевої мети: створення конфліктних ситуацій між окремими громадянами, розпалювання почуттів заздрості, підозри тощо.

Велику роль у руйнівній справі внесення розбрату та чвар в “Артхашастрі” відводиться вродливим молодим жінкам, які за допомогою підісланого агента повинні розпалювати ревнощі між конкурентами-чоловіками у будинках розпусти, сіючи чутки про невірність представниць слабкої статі, а також іншими способами, і пропонує, щоб під час любовних утіх вони вбивали своїх коханців, звинувативши згодом інших “потрібних” осіб, таким чином наразивши їх на смерть від руки “месників”. Жінок пропонувалося також використовувати й для інших провокацій, зокрема спочатку інтимної близькості, а згодом обвинувачення чоловіка у зґвалтуванні для подальшої компрометації, дискредитації і навіть створення приводу для фізичного усунення.

Висновки.

Розглянувши давньоіндійський трактат “Артхашастру”, переконуємося, що з найдавніших часів маніпулювання людьми, використання різних засобів інформаційно-психологічного впливу активно використовувалося у боротьбі з внутрішніми та зовнішніми противниками.

Одним із найбільш ефективних важелів досягнення кінцевої мети, за трактатом, є таємні операції, що реалізовувалися шляхом керованого інформаційного впливу на індивідуальну, групову або масову свідомість, волю громадян, їхні почуття. Для цього застосовувалося дезінформування суб’єктів ухвалення політичних і управлінських рішень, а також інші заходи, що мали на меті здійснювати негативний вплив на свідомість та настрої населення як держав противника, так і власних громадян. Свідомість, воля, почуття населення ставали об’єктами цільового ураження. У цій царині перевага віддавалася латентним і, здебільшого, підступним методам: поширенню

неправдивих чуток, дезінформуванню тощо, які за відсутності відповідних комунікативних технологій мали реалізовувати вже згадувані “шпигуни” й “агенти”.

Трактат висвітлює методи впливу на людей всупереч їх волі, зміни/формування психологічних установок, модифікації їх поведінки, обмеження свободи вибору, що необхідно враховувати у забезпеченні інформаційної безпеки.

На тлі вивчення історичного досвіду вкотре переконуємося, що інформаційна зброя здатна завдати відчутної шкоди стабільності будь-якої держави, позначитися не лише на житті громадянського суспільства, а й призвести до втрати державності, тому подальше вивчення проблеми забезпечення інформаційної безпеки та протидії негативним інформаційно-психологічним впливам є вкрай необхідною потребою сьогодення.

Використана література

1. Воеводин А.И. Стратагемы. Стратегия войны, манипуляции, бизнеса, обмана / А.И. Воеводин. – М. : Изд-во ИГ “Весь”, 2016. – 320 с.

2. Выдрин Дмитрий. Листая Артхашастру. – Режим доступу : http://vydrin.com/publications/articles/?id=446

3. Заяць Д. Індійський досвід управління персоналом : матеріали науково-практичної конференції за міжнародною участю [“Реформування системи державного управління та державної служби : теорія та практика”], (Київ, 8 квітня 2011 р.). – Ч. 2. – К., 2011 р. – С. 204-208.

4. Пиріг Роман. Дипломатія та зовнішня політика в “Артхашастрі”. – Режим доступу : http://uaforeignaffairs.com/ua/ekspertna-dumka/view/article/diplomatija-ta-zovnishnja-politika-v-artkhashastri

5. Мироненко О.М. Історія вчень про державу і право : навч. посібник / О.М. Мироненко, В.П. Горбатенко. – К. : ВЦ “Академія”, 2010. – 456 с.; Бонгард-Левин Г.М. Индия эпохи Маурьев. – М., 1973. – С. 120-149; История Востока ; отв. ред. В.А. Якобсон. – М., 1997. – Т. 1. – С. 418-423; Косамби Д. Культура и цивилизация Древней Индии. – М., 1968; Хрестоматия по истории Древнего Востока ; под ред. М.А. Коростовцева, И.С. Канцельсона, В.И. Кузищина. – М., 1980. – С. 75-111; Артхашастра, или Наука политики. – М. : Науч.-изд. центр “Ладомир”, 1993. – (Рос. акад. наук). – 793 с. – С. 539-542 с.; Древний Макиавеллизм : трактат “Артхашастра”. – Режим доступу : http://politology2004,narod.ru; Ирхин. Ю.В. Политическая мудрость Древнего Востока. – Режим доступу : http://pero-maat.narod.ru

6. Артхашастра или наука политики ; [пер. с санскрита] / издание подготовил В.И. Кальянов. – М.-Л. : Издательство Академии наук СССР, 1959. – 798 с.

7. ВЧК/ГПУ : документы и материалы ; ред.-сост. Ю.Г. Фельштинский. – М. : Издательство гуманитарной литературы, 1995. – 272 с.

8. Турло С. Шпионаж / С. Турло, И. Залдат. – М. : X-History, 2002. – 407 с.

9. В.С. Сідак. Спецслужба держави без території : люди, події, факти : (військова розвідка та контррозвідка ДЦ УНР в екзилі 1926-1936 рр.) / В.С. Сідак, Т.В. Вронська. – К. : Темпора, 2003. – С. 19-36.

10. Галузевий Державний архів СБ України. – Ф. 13. – Спр. 445.

11. Державний архів Російської Федерації. – Ф. 6215. – Оп. 1. – Спр. 10.

12. Центральний державний архів громадських об’єднань України. – Ф. 269. – Оп. 1. – Спр. № 184.

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

УДК 342.7:316.4

РАДЗІЄВСЬКА О.Г., старший науковий співробітник
НДІ інформатики і права НАПрН України

ІНФОРМАЦІЙНА ГРАМОТНІСТЬ ТА ЦИФРОВА НЕРІВНІСТЬ: УБЕЗПЕЧЕННЯ ДИТИНИ В СУЧАСНОМУ ІНФОРМАЦІЙНОМУ ПРОСТОРІ

Анотація. *Стаття присвячена дослідженню і вирішенню проблем інформаційної безпеки і способів убезпечення дитини від негативних інформаційних впливів. Надано пропозиції щодо удосконалення інформаційної грамотності та подолання цифрової нерівності в Україні.*

Ключові слова: *інформаційна грамотність, цифрова нерівність, інформаційна безпека, дитина.*

Аннотация. *Статья посвящена исследованию и решению проблем информационной безопасности и способов защиты ребенка от негативных информационных воздействий. Даны предложения по совершенствованию информационной грамотности и преодоления цифрового неравенства в Украине.*

Ключевые слова: *информационная грамотность, цифровое неравенство, информационная безопасность, ребенок.*

Summary. *This article is devoted to researching and solving information security problems and ways to safeguard the child from the negative impacts of information. The proposals are given for the improvement of information literacy and bridging the digital divide in Ukraine.*

Keywords: *information literacy, digital divide, information security, child.*

Постановка проблеми. Вимоги до інтелектуального розвитку індивідуумів в інформаційному суспільстві збільшуються, як збільшується і потреба у безпеці свідомості людини від різних видів інформаційних впливів. Безперешкодний і широкий доступ до інформації та знань є вкрай необхідною умовою життєдіяльності будь-якої людини, але ризики негативного впливу інформації надто великі у суспільстві, де “постістина” превалює над реальними фактами, а сприйняття добра і зла залежить від маніпулятивних модних трендів. Найбільш важливим суб’єктом у цьому аспекті виступають діти, на яких суспільством покладено функції здобування знань та акумулювання досвіду. Від того, наскільки якісно та ефективно пройде процес пізнання у дітей та їх подальша адаптація вимогам сьогодення, буде залежати їх особисте зростання, а також благополуччя держави та національна безпека, найважливішою складовою якої є інформаційна безпека.

Право на доступ до інформації є конституційним правом громадянина України, гарантується положенням статей 32 і 34 Конституції України [1] і регулюється законами України “Про інформацію” [2], “Про звернення громадян” [3], “Про доступ до публічної інформації” [4], “Про захист персональних даних” [5] та іншими нормативно-правовими актами. Згідно із Законом України “Про інформацію” [2] кожен має право на вільне одержання, використання, поширення, зберігання та захист інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

На початку 2007 року в Україні був прийнятий закон, який вперше визначив стратегічні напрями розвитку інформаційного суспільства в Україні, що передбачав, зокрема, “створення умов для забезпечення комп’ютерної та інформаційної грамотності

усіх верств населення” та “надання кожній людині можливості для здобуття знань, умінь і навичок з використання інформаційно-комунікаційних технологій (далі – ІКТ) під час навчання, виховання та професійної підготовки” [6]. В силу різних обставин, держава не змогла реалізувати його у повному обсязі у визначений час. Інформаційна грамотність населення в Україні все ще залишається вкрай низькою. Поряд із недостатньою інформаційною та комп’ютерною обізнаністю існує проблема нерівномірного доступу до інформації, знань та технологій різних соціальних груп. Так звана цифрова нерівність поряд із низьким рівнем інформаційної грамотності, особливо серед дітей, може призвести до втрати конкурентоспроможності держави в новому глобалізованому інформаційному світі та створить загрозу інформаційній безпеці громадян.

Аналіз досліджень. Проблемами інформаційної грамотності та цифрової нерівності в контексті доступу людини до інформації і знань, інформаційної безпеки та захисту персональних даних займалися такі видатні українські та зарубіжні вчені як І. Арістова, О. Баранов, К. Бєляков, В. Брижко, О. Дубас, М. Згуровський Р. Калюжний, О. Копан, І. Лук’янець, О. Марценюк, О. Олійник, В. Остроухов, В. Пилипчук, В. Петрик, С. Поленина, П. Прибутько, Н. Савінова, В. Фурашев, М. Швець та інші.

Проте предметна область, яка визначена у постановці завдання цієї роботи, потребує подальшого детального дослідження, що визначає її актуальність. Адже саме сьогодні формується інтелектуальний потенціал нашої нації, який безпосередньо впливатиме на забезпечення національної безпеки держави Україна у майбутньому. В умовах поширення активного застосування новітніх технологій типу Інтернет речей і “хмарних” технологій дедалі більшого значення набувають потреби якісної освіти, щоб якомога більше молоді здобувало потрібні навички щодо нового віртуального середовища, про що йде мова, зокрема в [7].

Метою статті є аналіз та визначення інформаційних викликів та загроз, що супроводжують трансформаційні процеси в нашій державі в контексті нерівномірності доступу дитини до інформації та знань.

Виклад основного матеріалу. Головною умовою добробуту кожної людини і держави в сучасному світі є знання, здобуті нею у безперешкодному доступі до інформації, обмін якою є необмеженим у просторі і часі. Інформація є першоджерелом та первинним ресурсом інформаційного суспільства. Проте сама по собі інформація, її кількість та широкий доступ до неї – це лише частина успішності сучасного індивідуума. Невід’ємною умовою для гармонійного та комплексного розвитку людини в сучасному суспільстві, її духовного та розумового збагачення є вміння якісно та швидко опрацьовувати здобуту інформацію, трансформувати її у нові знання та використовувати ці знання для систематизації та оброблення нових даних, а також впровадження накопичених знань у практичне застосування. Саме тому, на наш погляд, Д. Белл використовує поняття “знання” та “суспільство знань” а не “інформаційне суспільство” для характеристики сучасного суспільства, а нові здобутки постіндустріального суспільства пов’язує з переосмисленням інформації та інноваційним впровадження наново здобутих людством знань у практику [8]. За визначенням І. Кресіна та А. Колодюк знання – це “відтворення у свідомості людини характеристик речей, предметів, явищ дійсності, що переосмислені в категоріях людського досвіду”, а їх застосування підпорядковується певним правилам в залежності від ситуації, засобів та мети [9, с. 11]. Аналізуючи інформаційне суспільство далі вчені дійшли висновку, що за безперечності доступу всіх бажаючих до інформації та знань (крім випадків необхідного законодавчого обмеження)

вирішальним у новому суспільстві є здатність мислити та вміння використовувати інформацію [9, с. 8]. Зважаючи на динамічність розвитку сучасного суспільства, життя кожного індивідуума дедалі залежить від доступу до інформації та вміння пристосуватися до нових умов існування [10]. Тому для створення конкурентного національного людського капіталу та виховання високорозвинутого та високодуховного індивідуума державна політика в інформаційній сфері щодо своїх громадян повинна базуватися на таких основних принципах:

– максимального доступу до інформації, знань та надбань міжнародної спільноти;
– відсутності цифрової нерівності;
– можливості освоєння основних навичок та вмінь для роботи з інформацією та інформаційними ресурсами шляхом впровадження навчальних та освітніх програм;
– високого рівня інформаційної грамотності;
– високого рівня правосвідомості та відповідальної поведінки усіх суб’єктів інформаційної сфери;
– захищеності від негативного впливу інформації на свідомість та підсвідомість людини;
– уміння громадян створювати власний безпечний інформаційний простір.

Протягом усього життя людина накопичує інформацію. Починаючи від генетичної інформації, переданої від батьків, до поповнення її запасів у зрілому віці. Будь-який процес становлення особистості включає в себе надбання і засвоєння знань, накопичених людством в процесі еволюційного розвитку, здобуття навичок їх практичного застосування для власного і суспільного зростання та засвоєння основних принципів й механізмів суспільних взаємовідносин. Найважливішою ланкою у накопиченні знань з точки зору соціалізації людини є період її навчання в школі. Цей етап вважається надзвичайно важливим у формуванні особистості дитини та є найбільш насиченим в інформаційному плані. Адже саме в цей час основними функціональними обов’язками індивідуума, які на нього покладені суспільством, є накопичення та засвоєння знань. З іншого боку, для цього етапу дорослішання характерне активне залучення навчальних та освітніх інститутів держави на відміну від попереднього, де основну інформаційно-навчальну функцію було покладено на інститут батьківства.

Через швидкі темпи розвитку технологій освітянська сфера, яка звикла апелювати до досвіду та статистичних даних попередніх періодів, не встигає впроваджувати новинки у навчальний процес. Не встигає також із напрацюваннями нових методичних основ, хоча розуміння того, що система освіти потребує нового бачення, існує вже давно. Освітня система України дуже консервативна, а за відсутності достатнього фінансування, ще й досить неповоротка у впровадженні нових технологій в навчальний процес.

Сьогодні діти зростають в таких умовах, коли навчально-виховна система не охоплює тієї кількості інформації, яку вони отримують з оточуючого світу, є застарілою, малоадаптивною та ніби відірваною від повсякденного життя суспільства. Методи навчання, хоча і вкрай повільно, та все ж модернізуються. Впровадження нових технологій в учбовий та освітянський процес відбувається разом із дорослішанням й особистісним становленням дитини. Тому не існує чіткого розуміння правильності чи хибності цих кроків, немає результативних практичних напрацювань у цьому питанні. Загроза негативного інформаційного впливу на дітей сьогодні є вкрай актуальною і має тенденції до зростання. Це стосується не лише правильності впровадження нових технологій в учбовий процес, але й широкого залучення дитини до інформаційної сфери у позаучбовому повсякденному житті. Хоча діти значно швидше адаптуються до

сучасних умов, добре розуміються на сучасних технологіях, швидко навчаються та є успішнішими в освоєнні усього нового, проте є ряд аспектів, які викликають занепокоєння у фахівців з інформаційної безпеки дитини.

У 2007 році у Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” було визнано, що надто повільне впровадження нових методів навчання із застосуванням сучасних ІКТ заважає досягнути достатнього рівня інформаційної грамотності населення і є однією із причин, які заважають рухатись країні вперед у розбудові інформаційного суспільства. На жаль, слід констатувати, що ситуація мало змінилася з часу прийняття цього закону, хоча однією із стратегічних цілей держави було саме “забезпечення комп’ютерної та інформаційної грамотності населення, насамперед шляхом створення системи освіти, орієнтованої на використання новітніх ІКТ у формуванні всебічно розвиненої особистості” та “захист інформаційних прав громадян” [6].

Сьогодні спостерігається хаотичність та ситуативність модернізації системи освіти.

Якщо школи у містах, зокрема гімназії, ліцеї, можуть похвалитись не лише забезпеченням комп’ютерами усіх учнів, але й створенням власних мереж, навчальних та методичних баз даних, електронних щоденників, системи електронного відвідування, тощо, то у сільській школі – заледве є декілька комп’ютерів, а про підключення їх до мережі Інтернет мова взагалі не йде. За даними матеріалів аналітичної доповіді Д. Дубова та М. Ожевана “Широкосмуговий доступ до мережі Інтернет, як важлива передумова розвитку України” станом на 2013 р. в українських містах із населенням понад 10 тис. чоловік, лише 5 – 7 % мешканців мали доступ до мережі Інтернет через оптоволоконний кабель, а в сільській місцевості така ситуація була ще гіршою [11]. Тоді як у Стратегії сталого розвитку “Україна – 2020”, схваленої Указом Президента України від 12 січня 2015 року № 5/2015, в контексті розбудови “інформаційного суспільства та медіа” в Україні (п. 4 с. 3) передбачається, що “частка проникнення широкосмугового Інтернету за даними Світового банку складатиме 25 абонентів на 100 осіб” (п. 18 с. 4) [12].

Ще одним підтвердженням цифрової нерівності в Україні є дослідження компанії Gemius. За даними цього дослідження аудиторія українського Інтернету за 2014 рік зросла на 12 %. Зокрема, найбільший приріст користувачів Інтернету спостерігається у містах з населенням більше 500 тис. – 35,7 %, у містах з населенням 101 - 500 тис. – 24,2 %, менше 100 тис. – 21,1 %, і найменше збільшення кількості інтернет-користувачів у селах – 19,1 %. Тенденції до регіонізації росту інтернет-аудиторії: чим більше місто, тим інтенсивніше розвиваються у ньому технології – зберігаються й надалі [13]. Залученість користувачів до мережі Інтернет за регіонами України та віковими характеристиками представлена далі у Таблиці.

Дані дослідження отримані компанією Factum Group Ukraine на замовлення Інтернет Асоціації України (N=2097, вся Україна до 2014 року, без АР Крим після 2014 року , вік 15+) [14].

Аналізуючи представлені дослідження, можна стверджувати, що сьогодні ситуація з забезпечення доступу до інформації і знань, представлених у всесвітній мережі, дещо покращилась, проте – не значно. Якщо ще рік назад користувачів Інтернету у селах було 36 % то за рік їх приріст склав 11 %, тоді як у містах понад 100 тис. – лише 2 %. Регіональні тенденції охоплення споживачів Інтернетом зберігається. Що вказує на те, що можливість повноцінного доступу до світового надбання інформації і знань в Україні диференційована за територіальними особливостями її мешканців. Традиційно найбільш активними користувачами мережі

є наймолодші серед опитаних, тобто люди до тридцяти років. Їх охопленість наближається до 100 %. Якщо говорити про підлітків, то вони є найактивнішими у віковій групі до 30 років. Тобто найбільш охопленою категорією користувачів Інтернету є молодь великих міст.

Таблиця

Динаміка залученості населення до мережі Інтернет
(кількість користувачів, що користуються Інтернетом 1 раз на місяць і частіше).

	2011 рік	**2012 рік**	**3013 рік**	**2014 рік**	**2015 рік**	**2016 рік**
За регіонами, % :						
село	18	21	36	36	36	47
місто до 100 тис.	34	39	51	56	61	55
місто більше 100 тис.	55	56	65	65	67	69
За віком, % :						
15-29 років	70	74	85	86	91	92
30-44 років	45	56	68	74	79	86
45-54 років	24	32	41	51	61	65
55+ років	5	7	42	36	42	47

Проводячи аналіз та співставлення даних дослідження, можемо зробити висновок, що в Україні склалася ситуація, коли її мешканці, громадяни з рівними конституційними правами мають різні можливості для доступу до інформації та знань в залежності від місця проживання.

Іншим фактором нерівності у доступі до інформації і знань є соціальна нерівність громадян України. Розрив між доходами найбагатших та найбідніших українців залишається великим, а кількість родин з мінімальним рівнем достатку є все ще значною. Таким чином, виникає нерівномірність у доступі до інформації і знань дітей різних соціальних груп та різних регіонів України. Така ситуація значно поглиблює “інформаційну нерівність” між окремими регіонами та верствами населення. За такої цифрової нерівності діти окремих категорій зазнають дискримінації в інформаційній сфері, що суперечить нормам міжнародного та національного права. Саме соціальна нерівність, на думку О. Баранова, породжує цифрову нерівність. Серед основних чинників, що впливають на доступ до інформації та знань, є, насамперед, економічне становище, освітній рівень, вік, місце проживання [15].

Ще одним аспектом цифрової дискримінації дітей з різних регіонів та соціальних груп є їх рівень навичок та вмінь для роботи з інформацією. Це пов’язано з низьким фаховим рівнем викладачів у звичайних школах в порівнянні з рівнем викладання в спеціалізованих навчальних закладах. У невеликих школах є практика заміщення викладачів окремих предметів непрофільними викладачами за суміщенням. Наприклад, викладача інформатики, як правило, у таких школах взагалі немає, а предмет викладається іншим педагогом, що не має достатніх знань та навичок. Такий підхід докорінно нівелює прагнення держави у русі до інформаційного суспільства. У результаті діти не отримують достатніх знань, умінь знаходити, виокремлювати і використовувати необхідну інформацію для власних потреб, не мають навичок у сфері

роботи з сучасними інформаційними ресурсами і технологіями, не вміють убезпечувати власний інформаційний простір. А відтак, такі діти не зможуть досягти такого ж інтелектуального рівня як їх однолітки-гімназисти (чи ліцеїсти), тобто зазнають соціальної дискримінації та залишаються беззахисними перед загрозами інформаційного простору.

Така нерівність не лише створює дискримінацію окремих категорій громадян за можливістю доступу до інформації і знань, а й становить загрозу нерівності щодо рівня інтелектуального розвитку між дітьми великих міст та сіл, учнів звичайних та спеціалізованих освітніх закладів. Не маючи повноцінного доступу до інформації, знань, технологій та вмінь працювати з ними сільські діти, чи учні звичайних шкіл не зможуть досягти такого ж високого інтелектуального рівня, як їх однолітки з великих міст, чи ліцеїв (гімназій), не вмітимуть повноцінно використовувати сучасні ІКТ, адаптуватися до вимог нового суспільства, що засноване на широкому впровадженні інформаційних та інноваційних технологій, та стати повноцінними його членами. Такі категорії дітей слід було б віднести до групи ризику з підвищеним рівнем інформаційної віктимності.

Інформаційна нерівність, накладаючись на соціальну нерівність, призводитиме до віктимізації суспільства та підвищення індивідуальної та групової віктимності у дітей окремих груп, і не лише в інформаційній сфері.

Зважаючи на те, що за даними статистики кількість сільських мешканців складає третину від загальної кількості мешканців Україні, а приріст населення у сільській місцевості більший за приріст у містах (12,6 осіб на 1000 осіб проти 10,9 у міських поселеннях) [16] та враховуючи трудову міграцію молоді з України у країни Європи та США – можемо стикнутися з проблемою зниженням загального інтелектуального рівня в державі та її конкурентоспроможності, що у подальшому призведе до сповільнення розвитку інформаційного суспільства в Україні загалом. Такі виклики можуть становити загрозу національній безпеці України у майбутньому.

Рівність прав дітей в Україні незалежно від їх походження гарантовано ст. 52 Конституції України [1]. Також, за Конституцією України держава гарантує дітям право на безкоштовну освіту (ст. 53) та можливість “вільно збирати, зберігати, використовувати та поширювати інформацію усно, письмово, або в інший спосіб – на свій вибір” (ч. 2 ст. 34).

На міжнародному правовому рівні проблема рівності можливостей дітей зачіпалася ще у 1959 р. У ст. 7 Декларації прав дитини зазначено, що дитина має право на безкоштовну освіту, яка сприяла б її загальному культурному розвитку і завдяки якій вона могла б, *на основі рівності можливостей*, розвивати свої здібності та особисті судження, відчуття моральної та соціальної відповідальності [17]. Ці принципи були розширені та доповнені у Конвенції про права дитини (далі – Конвенція) [18], яка була ратифікована Україною у 1991 році. Зокрема, у ст. 28 Конвенції визнається право дитини на освіту і *на підставі рівних можливостей* серед іншого держави-учасниці “забезпечують доступність інформації і матеріалів у галузі освіти й професійної підготовки для всіх дітей” (пп. d п. 1 ст. 28) і створюють можливості для “полегшення доступу до науково-технічних знань і сучасних методів навчання” (п. 3 ст. 28). Стаття 13 Конвенції, перекликаючись із ст. 34 Конституції України, дає право дитині “вільно висловлювати свої думки …шукати, одержувати і передавати інформацію та ідеї будь-якого роду незалежно від кордонів в усній, письмовій чи друкованій формі, у формі творів мистецтва чи за допомогою інших засобів на вибір дитини”, а ст. 17 покладає на державу-учасницю функції по

забезпеченню доступу дитини “до інформації і матеріалів із різних національних і міжнародних джерел, особливо до таких інформації і матеріалів, які спрямовані на сприяння соціальному, духовному і моральному благополуччю, а також здоровому фізичному і психічному розвитку дитини”. І нарешті, ст. 2 Конвенції зобов’язує держав-учасниць вживати “всіх необхідних заходів для забезпечення захисту дитини від усіх форм дискримінації”.

Сьогодні в Україні планується проведення адміністративно-територіальної реформи, яка передбачає передання частини повноважень та коштів на місця. Зокрема, за новими нормами заклади загальної середньої освіти передаються до компетенції місцевих органів влади, а їх фінансування здійснюватиметься не з державного, а з місцевих бюджетів. Оскільки наповнення місцевого бюджету залежить від специфіки регіону, то й відповідно фінансування навчальних закладів різних регіонів буде різним. У більш багатому регіону фінансування закладів освіти буде більшим, ніж у бідному, депресивному регіоні. Виникає загроза того, що освітні заклади деяких регіонів України будуть фінансуватись не в повному обсязі, а відтак, не зможуть повноцінно розвиватись, впроваджувати нові технології в освітянський процес та надавати високий рівень знань дітям. Зважаючи на уже існуючі проблеми матеріально-технічного та кадрового забезпечення шкіл окремих регіонів, держава Україна найближчим часом може стикнутися з серйозним викликом її інформаційній безпеці та інформаційній безпеці її громадян. Тому уже сьогодні необхідно передбачити компенсаційні механізми для забезпечення рівності доступу дітей різних регіонів до інформації та знань, можливості отримання високого рівня освіти в незалежності від регіону проживання. Оскільки освіта належить до сфери інтересів держави та є об’єктом її національної безпеки, то координація діяльності в ній має теж здійснюватися на державному рівні. Зважаючи на серйозність змін у державі найближчим часом, виникає необхідність врахування ряду ключових моментів щодо освіти у перехідних положеннях нового закону “Про адміністративно-територіальний устрій України” у розділі “Освіта”. Необхідно передбачити єдиний освітній стандарт високого рівня, обов’язковий до виконання усіма без винятку закладами освіти, незалежно від форми підпорядкування та власності. Також необхідний єдиний державний орган контролю за дотриманням цих норм. Для вирівнювання можливостей у наданні освітніх послуг навчальними закладами різних регіонів необхідно розробити систему цільових грантів, що дозволила б підтримувати школи бідних регіонів.

Очевидно, що навчання у школі – це той період життя дитини, на який державі потрібно звернути особливу увагу, бо саме у цей період особа не тільки накопичує інформацію, але й отримує основні навички роботи з нею, вміння її знаходити, аналізувати, обробляти, накопичувати та трансформувати у необідні знання і навички. Тому перед науковою та освітньою спільнотою сьогодні стоїть дуже важливе питання належного рівня підготовки підростаючого покоління, щоб воно стало конкурентоспроможним у новому, видозміненому світі. Вміння виокремити з надзвичайно великої кількості інформації необхідну, трансформувати її у знання та у подальшому вдало її використати стає необхідною умовою для благополучного існування у майбутньому. Інтелектуальний потенціал людини сьогодні є найважливішим. Вважається, що для збільшення промислового потенціалу держави у два рази необхідно збільшити інтелектуальний потенціал в чотири [19, с. 73; 20, с. 17]. З іншого боку, інформаційна безпека як суспільства, так і кожного громадянина, а також їх вміння протистояти негативним інформаційним впливам на

свою свідомість та підсвідомість залежить від рівня інтелектуальності, спеціальної теоретичної й практичної підготовки; критичного мислення, морального та духовного вдосконалення; гармонійного розвитку особистості в суспільстві [21, с. 122; 22, с. 122; 23, с. 70-82]. Тому проблема інформаційної грамотності тісно пов’язана з питаннями інформаційної безпеки особи у новому суспільстві та є на сьогодні надзвичайно актуальною. Нехтування інформаційною безпекою у суспільстві сьогодні не дозволить сформувати здорове та прогресивне суспільство завтра. Адже лише повноцінний доступ до достовірної інформації та знань, відсутність маніпулювання свідомістю дитини, закладання вірних мессиджів, направлених на формування національних та загальнолюдських цінностей, формування правосвідомості дасть можливість виростити гармонійну особистість, здатну до самореалізації та самовдосконалення. Саме така особистість здатна рухати економіку країни уперед.

Зволікання держави у питаннях підвищення інтелектуального потенціалу та формування у суспільстві сталого людського потенціалу, націленого на прогрес та розвиток, при достатньому рівні убезпечення її в інформаційному просторі може призвести до втрати конкурентоспроможності держави, що не дозволить їй повноцінно розвиватись та забезпечувати достойний рівень життя її громадян.

Збільшення обсягу інформації та кількості комунікативних зв’язків, формування медіасвідомості (кліповості сприйняття) у дитини спонукає до фрагментарності у сприйнятті світу, кризи самоідентифікації особистості, соціальних груп, втрати або трансформації сталих міжлюдських, міжнаціональних, міждержавних та інших суспільних зв’язків. На цьому акцентують увагу у своїх роботах такі вчені як М. Згуровський, І. Жиляєв, О. Копан, О. Марценюк, С. Поленіна М. Родіонов, М. Швець [20, с. 17; 24, с. 19] і вбачають небезпеку подальшого розвитку інформаційного суспільства у наростанні різних форм нерівності між людьми як на глобальному, так і на національному рівнях. Єдиним виходом вважається напрацювання єдиних норм та правил поведінки у глобальному масштабі [20, с. 17; 25, с. 17; 19, с. 63-65].

Отже, інформаційна грамотність та інтелектуальний потенціал особи є необхідною умовою індивідуального та суспільного розвитку, зростання конкурентоспроможності держави, водночас, будучи невід’ємною складовою індивідуальної та національної безпеки в інформаційній сфері.

Інформаційна безпека особи і суспільства є іншою стороною медалі і також залежить від інформаційної грамотності та доступу громадян до інформації і знань. Як стверджують фахівці рівень інформаційної безпеки особи залежить від рівня обізнаності індивідуума з реальними та потенційними загрозами в інформаційному суспільстві та його інтелектуальним рівнем [22, с. 122].

Із трьох структурних елементів інформаційної безпеки особи, виділених О. Олійником [26, с. 133], загрози у сфері основних прав і свобод людини, до яких і віднесений безперешкодний та повний доступ до інформації і знань, є першим та основним пунктом поряд із загрозами інформаційно-психологічній безпеці особи і суспільства (2) та загрозами “з використанням інформаційно-технічних засобів” (3). Такої думки притримується і О. Баранов, виділяючи у пункт перший складових інформаційної безпеки особи “…неповноту, невчасність та невірогідність інформації, що використовується” [27, с. 30-34].

Не можливо не погодитись із твердженнями українських науковців, що будь-яка особа має сприйматись як індивідуальність, а на її дії можна впливати тільки шляхами

заохочення, переконання, особистої зацікавленості, а не засобами наказів чи примусу тоталітарної волі держави або колективу [20, с. 33] Це є вкрай актуальним в інформаційній сфері, де будь-яка заборона чи обмеження призводять до шаленого супротиву, перекручування ситуації та маніпулювання зі свідомістю населення. Тому принцип індивідуального переконання методом зацікавленості, а не примусу повинен лягти в основу нової концепції системи освіти та методики навчання.

Висновки.

Підсумовуючи викладене, можна стверджувати:

- система освіти в Україні не відповідає сучасним потребам суспільства, не створює задовільні умови для вільного доступу дітей до інформації та знань, не забезпечує достатнього рівня їх обізнаності та породжує інформаційну нерівність серед дітей різних соціальних груп та за територіальними ознаками. Інформаційна нерівність у доступі до інформації та знань, необхідних для навчання та повноцінного розвитку дитини, є неприпустимою, призводить до дискримінації та суперечить нормам національного та міжнародного права;
- одним з головних завдань держави у сфері забезпечення інформаційної безпеки людини, а особливо дитини, є забезпечення належного інтелектуального рівня, обізнаності населення щодо інформаційних загроз та переконання у необхідності дотримання ними правил безпечної поведінки в інформаційному просторі. Прогресуючий сьогодні нігілізм в інформаційному просторі повинен поступитися під натиском правоосвіти і сформувати правосвідому особистість з високим рівнем медіа- та Інтернет-грамотності та суспільної відповідальності. Забезпечення інтелектуального зростання та обізнаності у державі покладено на інститути соціалізації, зокрема на навчальні заклади. Проте сучасне суспільство є перехідним суспільством. Йому притаманні системні зміни, у тому числі, й трансформаційні процеси у навчальній та виховній сферах;
- з метою створення умов для реалізації прав дитини в інформаційній сфері, гарантованих національним законодавством та міжнародним правом, зокрема, ст. ст. 34, 52, 53 Конституції України, принципом 7 Декларації прав дитини, ст. 2, пп. d п. 1, п. 3 ст. 28 та ст. 17 Конвенції про права дитини, подолання цифрової нерівності серед дітей, а також враховуючи сучасний рівень викликів і загроз їх інформаційній безпеці необхідно консолідувати зусилля держави, приватного сектору та громадянського суспільства у таких основних напрямах:
  - забезпечення потенційної можливості універсального доступу дітей до інформації та сучасних навчальних ресурсів шляхом розвитку інформаційної інфраструктури та створення навчально-освітніх центрів при школах, бібліотеках, будинках дітей та юнацтва;
  - забезпечення можливості здобуття необхідних знань, вмінь та навичок використання новітніх інформаційно-комунікативних технологій для одержання інформації та знань;
  - забезпечення можливості отримання необхідних знань щодо існуючих чи потенційних загроз, інформаційної безпеки та вмінь убезпечувати власний інформаційний простір;
  - проводити процес соціалізації дитини з врахуванням нових чинників впливу на формування особистості та її комунікативних навичок.

На підставі вищевикладеного, уявляється за доцільне розглянути питання щодо: розроблення Державної цільової освітньої програми “Освіта майбутнього” на період до 2020 року, у якій передбачити:

- створення рівних можливостей у доступі до інформації і знань для усіх дітей, незалежно від місця проживання і соціального статусу;
- підвищення рівня правосвідомості, правової та інформаційної культури у дітей шляхом імплементації у навчальний курс “Правознавство” основ інформаційного права та правових механізмів регулювання суспільних відносин в інформаційній сфері;
- впровадження у навчальний процес дисципліни “Інформаційна безпека”, як окремого предмета, або його викладання у складі дисципліни “Основи життєдіяльності”;
- удосконалення методик викладання курсу “Інформатика” у шкільній програмі для підвищення комп’ютерної та інформаційної грамотності дітей з урахуванням сучасних викликів і загроз в інформаційній сфері;
- облаштування бібліотек безпечним широкосмуговим з’єднанням із мережею Інтернет з метою розширення можливостей доступу дітей до національних духовних, культурних та історичних цінностей, досягнень світової культури і науки відповідно до статті 20 Закону України “Про охорону дитинства” [27];
- створення у комп’ютерних класах навчальних закладів достатньої кількості робочих місць, обладнаних сучасною технікою і програмним забезпеченням із безпечним широкосмуговим доступом до мережі Інтернет, для оволодіння новими технологіями і здобуття навичок їх практичного використання у процесі пізнання й накопичення знань;
- проведення заходів національного і патріотичного виховання молоді в контексті протидії маніпулятивним інформаційно-психологічним впливам на дітей.

Також вважаємо за доцільне, під час проведення в Україні адміністративно-територіальної реформи, коли повноваження та кошти будуть передані на місця, передбачити систему цільових грантів для навчальних закладів депресивних регіонів, задля недопущення збільшення розриву у доступі до інформації між дітьми великих міст і маленьких селищ та сповільнення чи згортання програм модернізації системи освіти. Щоб не допустити в Україні поглиблення інформаційної нерівності, слід разом із запровадженням адміністративно-територіальної реформи чітко прописати єдині стандарти освіти по всій території країни та створити систему органів, що будуть її забезпечувати та контролювати. Оскільки освіта належить до пріоритетних напрямів розвитку держави та до сфери державних інтересів, у тому числі й національної безпеки, необхідно забезпечити достатній рівень фінансування усіх навчальних закладів незалежно від можливостей місцевого бюджету. Це дозволить позбутися інформаційної нерівності, дискримінації дітей різних соціальних груп та забезпечити високий інтелектуальний рівень підростаючого покоління, що стане запорукою процвітання нашої держави у майбутньому.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-D0%B2%D1%80

2. Про інформацію : Закон України від 02.10.92 р. № 2657-XII ВР. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2657-12

3. Про звернення громадян : Закон України від 02.10.96 р. № 393/96-ВР. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/393/96-%D0%B2%D1%80

4. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2939-17

5. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/2297-17

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

7. Програма Internet of Things у Львівській політехніці чекає абітурієнтів. – Режим доступу : http://itcluster.lviv.ua/programa-internet-things-u-l-vivs-kij-politehnitsi-chekaye-abituriyentiv

8. Bell D. The Third Technological Revolution and Its Possible Socio-Economic Consequences // Dissent. Vol. XXXVI. No 2. Spring 1989. – P. 167.

9. Правове забезпечення інформаційної діяльності в Україні ; за заг. ред. Ю.С. Шемшученка, І.С. Чижа. – К. : ТОВ “Видавництво “Юридична думка”, 2006. – 384 с. – С. 11.

10. Дубас О. Інформаційний розвиток сучасної України у світовому контексті : політологічний аналіз : дис. на здобуття наук. ступеня канд. політ. наук : 23.00.02. – К., 2004. – С. 74-75.

11. Дубов Д.В. Широкосмуговий доступ до мережі Інтернет як важлива передумова розвитку України : аналіт. доп. / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2013. – С. 58.

12. Про Стратегію сталого розвитку “Україна – 2020” : Указ Президента України від 12.01.15 р. № 5/2015. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/5/2015

13. Аудиторія українського Інтернету сповільнила свій ріст – за рік зросла лише на 12 % ; (за 19 серпня 2014 р.). – Режим доступу : http://watcher.com.ua/2014/08/19/audytoriya-ukrayinskoho-internetu-spovilnyla-sviy-rist-za-rik-zrosla-lyshe-na-12

14. Мінченко О. Проникнення Інтернету в Україні вперше перевищило 60 % / “Watcher” ; (за·28 березня 2016 р.) – Режим доступу : http://watcher.com.ua/2016/ 03/28/pronyknennya-internetu-v-ukrayini-vpershe-perevyschylo-60. – Назва з титул. екрана. – (Дата звернення : 02.05.2016).

15. Баранов А.А. Преодоление цифрового неравенства – путь к построению информационного общества в Украине : зб. аналітич. доповід. “Свобода інформації, прозорість, електронне врядування: погляд громадянського суспільства” ; за ред. А.В. Пазюка. – К. : МГО “Прайвесі Юкрейн”, 2004. – 206 с. – С. 73-90.

16. Населення України. – Режим доступу : https://uk.wikipedia.org/wiki/%D0%9D%D0%B0%D1%81%D0%B5%D0%BB%D0%B5%D0%BD%D0%BD%D1%8F_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8#cite_note-ukrstat1-8. – Назва з титул. екрана. – (Дата звернення : 12.03.2016).

17. Международная защита прав и свобод человека. Права человека : сборник международных договоров. – М. : Юридическая литература, 1990. – С. 139-141.

18. Конвенція про права дитини : Міжнародний документ ООН від 20.11.1989 року. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_021

19. Поленина С.В. Правовая система в условия глобализации и региональной интеграции : теория и практика ; отв. ред. С. В. Поленина. – М. : Формула права, 2006. – 558 с.

20. Теоретико-методологічні засади інформаційного права України : реалізація права на інформацію : монографія / [Р.А. Калюжний, О.В. Копан, О.Г. Марценюк]. – К. : “МП Леся”, 2013. – 236 с.

21. Петрик В.М. Сутність інформаційної безпеки держави, суспільства та особи // Юридичний журнал. – 2009. – № 5. – С. 122-134.

22. Прибутько П.С. Інформаційні впливи : роль у суспільстві та сучасних воєнних конфліктах / П.С. Прибутько, І.Б. Лук’янець. – К. : ПАЛИВОДА А.В., 2007. – 252 с.

23. Брижко В. е-боротьба в інформаційних війнах та інформаційне право : монографія / В. Брижко, М. Швець; за ред. М. Швеця. – К. : ТОВ “ПанТот”, 2007. – 218 с.

24. Вступ до інформаційної культури та інформаційного права / [М.Я. Швець, Р.А. Калюжний та ін.] ; за заг. ред. М.Я. Швеця, Р.А. Калюжного. – Ужгород : ІВА, 2003. – 240 с.

25. Згуровський М.З. Розвиток інформаційного суспільства в Україні : правове регулювання в сфері інформаційних відносин / М.З. Згуровський, М.К. Родіонов, І.Б. Жиляєв. – К. : НТТУ “КПІ”, 2006. – 542 с.

26. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки в Україні // Право і суспільство. – 2012. – № 3. – С. 132-137.

27. Баранов О.А. Базові принципи інформаційного права – забезпечення інформаційної безпеки : матеріали наук.-практ. конф. [“Запобігання новим викликам і загрозам інформаційній безпеці України : правові аспекти”], (Київ, 6 жовтн. 2016 р.) ; упоряд. В.М. Фурашев. – К. : НТУУ “КПІ ім. Ігоря Сікорського”, Вид-во “Політехніка”, 2016. – 204 с.

28. Про охорону дитинства : Закон України від 26.04.01 р. № 2402-III. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2402-14

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

УДК 351.86:351/354+004.056

ДОРОНІН І.М., *кандидат юридичних наук, доцент*

ПРАВОВЕ РЕГУЛЮВАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ У РЕАЛІЗАЦІЇ ОКРЕМИХ ФУНКЦІЙ ДЕРЖАВИ

Анотація. *У статті на підставі аналізу документів стратегічного планування держави, актів законодавства та проектів законодавчих актів, досліджено питання реалізації окремих функцій держави у формі правового регулювання забезпечення кібербезпеки.*

Ключові слова: *кібербезпека, стратегічне планування, оборона, забезпечення державної безпеки, реалізація функції держави.*

Аннотация. *В статье на основании анализа документов стратегического планирования государства, актов законодательства и проектов законодательных актов, исследован вопрос реализации отдельных функций государства в форме правового регулирования обеспечения кибербезопасности.*

Ключевые слова: *кибербезопасность, стратегическое планирование, оборона, обеспечение государственной безопасности, реализация функции государства.*

Summary. *This article explores the issue of implementation of state functions by the legal regulation of cybersecurity based on the analysis of the state strategic planning documents, current legislation, draft laws in the field of cybersecurity.*

Keywords: *cybersecurity, strategic planning, defense, state security, the implementation of state functions.*

Постановка проблеми. У сучасних умовах фактичної гібридної війни, яка ведеться проти України, питання забезпечення кібербезпеки у нашій державі має надзвичайно велике значення. Ужиття заходів, визначених Стратегією національної безпеки України, затвердженою Указом Президента України від 26.05.15 р. № 287/2015 та Стратегією кібербезпеки, затвердженою Указом Президента України від 15.03.16 р. № 96/2016, зумовило необхідність змін у чинному законодавстві, насамперед з метою подальшого унормування суспільних відносин, пов’язаних з реалізацією таких функцій держави, як оборона та забезпечення державної безпеки.

На розвиток цього за останній рік було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14.03.16 р. № 92/2016, Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 06.06.16 р. № 240, Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 07.06.16 р. № 242/2016, Порядок формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23.08.16 р. № 563 та низка інших.

Як показує аналіз зазначених актів, переважна більшість з них встановлює загальні засади державної політики і визначає окремі підходи до унормування питань забезпечення кібербезпеки. Водночас, деякі заходи та стратегічні підходи не повною мірою базуються на науковому підґрунті, що неодмінно призведе до неналежного правового регулювання суспільних відносин, виникнення спірних питань стосовно застосування правових норм.

Аналіз основних досліджень і публікацій. Питання правової регламентації забезпечення кібербезпеки та її організаційних основ були предметом численних наукових публікацій за останні роки як вітчизняних [1 – 9], так і іноземних [10 – 14] дослідників. Водночас, практично відсутні публікації стосовно проблемних питань правого регулювання забезпечення кібербезпеки у контексті реалізації функцій держави. Крім цього, основний масив наукових напрацювань зосереджено навколо з’ясування термінологічної бази, визначення відповідних дефініцій або дослідження особливостей кримінальної відповідальності за вчинення злочинів з використанням інформаційно-телекомунікаційних систем.

Метою статті є проведення аналізу вітчизняної нормативно-правової бази, доктринальних документів та документів стратегічного планування держави останнього часу, дослідження впливу форм реалізації окремих функцій держави на стан правового регулювання, організацію і планування відповідних організаційних заходів.

Виклад основного матеріалу. Після ухвалення 20 грудня 2002 року Генеральною асамблеєю ООН резолюції 57/239 “Елементи для створення глобальної культури кібербезпеки” зазначений термін почав активно використовуватись у вітчизняній правовій термінології. Складніше було з імплементацією змісту резолюції. Зокрема, Генеральна асамблея ООН констатувала, що стрімкий розвиток інформаційної технології означає зміну підходів державних органів, організацій та індивідуальних користувачів до питання кібербезпеки.

За цих умов було визначено дев’ять взаємопов’язаних елементів, а саме:

- *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що саме 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 виявлення та реагування, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективне співробітництво з метою попередження, виявлення та реагування таки інцидентів;
- *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 і практику забезпечення безпеки з урахуванням виникнення нових та зміни існуючих загроз).

У подальшому правове регулювання вжиття заходів з кібербезпеки (окрім деяких суто кримінально-правових аспектів) в Україні в основному було зумовлено вимогами євроатлантичної інтеграції держави і випливало з доктрин, стратегій та настанов НАТО і Євросоюзу.

Зокрема, у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12.02.07 р., стан безпеки інформаційно-комп’ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій охарактеризовано як такий, що наближається до критичного. А у подальшому в п. 4.1 зазначеної Стратегії з метою реалізації державної політики було визнано за необхідне розробку та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність. Слід зазначити, що запропонований у першій редакції Стратегії національної безпеки підхід, який з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов’язань та вимог гармонізації законодавства до європейських стандартів, був цілком адекватним обстановці та повністю відповідав елементам для створення глобальної культури кібербезпеки, визначеним резолюцією Генеральної асамблеї ООН.

У подальшому Указом Президента України від 08.06.12 р. № 389/2012 було затверджено нову редакцію Стратегії національної безпеки України “Україна у світі, що змінюється”. Цей документ доктринального характеру, характеризуючи безпекове середовище, серед чинників впливу на національну безпеку визначав нездатність держави протистояти викликам, пов’язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. Чинна на той час редакція ст. 8 Закону України “Про основи національної безпеки України” серед загроз в інформаційній сфері визначала:

- прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп’ютерна злочинність та комп’ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Таким чином, зазначені новітні виклики та загрози фактично не було визначено на рівні документів стратегічного планування, оскільки комп’ютерна злочинність та комп’ютерний тероризм далеко не повністю охоплюють такі загрози.

Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково було зазначено:

- стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;
- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об’єктами критичної інфраструктури;
- створення національної системи кібербезпеки.

І нарешті, у чинній редакції Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287/2015, серед загроз інформаційній безпеці визначено:

• ведення інформаційної війни проти України;

• відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства.

Загрозами кібербезпеці і безпеці інформаційних ресурсів є:

• уразливість об’єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;

• фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Отже, у чинній Стратегії національної безпеки України характеристику загроз кібербезпеці обмежено, а фактично зведено до кібератак та застарілості системи охорони інформації з обмеженим доступом. З іншого боку визначення як окремої загрози ведення інформаційної війни проти України розширило поле, яке характеризує загрози у кіберпросторі.

Формулюючи основні напрями державної політики щодо забезпечення кібербезпеки та інформаційної безпеки, внаслідок розділення цих сфер безпеки, не вдалося уникнути певного дуалізму і у формулюванні напрямів політики. Зокрема, створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них і моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації є багато у чому пов’язаними заходами. До того ж розвиток інформаційної інфраструктури держави стосується не тільки забезпечення кібербезпеки, а й інформаційної безпеки також.

У подальшому основні напрями державної політики забезпечення саме кібербезпеки було окреслено у Стратегії кібербезпеки України, яку затверджено Указом Президента України від 15.03.16 р. № 96/2016. Метою цієї Стратегії визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Як показує аналіз пріоритетів та напрямів державної політики щодо забезпечення кібербезпеки, які визначені у розділі 4 Стратегії кібербезпеки, переважна більшість з них стосуються організаційних заходів, що є взаємопов’язаними і повинні складати відповідну систему забезпечення кібербезпеки. У питанні вжиття заходів правового регулювання забезпечення кібербезпеки Стратегією визнано за доцільне необхідність приведення вітчизняного законодавства у відповідність до вимог НАТО та ЄС, комплексне вдосконалення правової основи кіберзахисту об’єктів критичної інфраструктури, подальший розвиток кримінально-правової охорони суспільних відносин у цій сфері, боротьба з кіберзлочинністю.

На виконання Стратегії кібербезпеки України розпорядженням Кабінету Міністрів України від 24.06.16 р. № 440-р було затверджено план заходів на 2016 рік з реалізації зазначеної Стратегії. У цій статті неможливо провести аналіз стану здійснення державними органами положень зазначеного плану. Скоріше за все його виконання було незадовільним. Тому рішенням Ради національної безпеки і оборони України від 29.12.16 р., уведеним в дію Указом Президента України від 13.02.17 р. № 32/2017, акцентовано увагу на необхідності термінової підготовки законодавчих пропозицій щодо кіберзахисту об’єктів критичної інформаційної інфраструктури, посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах та законних вимог посадових осіб органів Державної служби спеціального зв’язку та захисту інформації України, а також щодо запровадження відповідальності за невиконання законних вимог посадових осіб Служби безпеки України розробки низки правових новел у сфері кібербезпеки.

Слід зазначити, що більшість з перелічених питань є предметом правового регулювання у проекті Закону України “Про основні засади забезпечення кібербезпеки України”, який було прийнято Верховною Радою України за основу 20.09.16 р. Проте, зазначений проект далекий від досконалого, на що справедливо було звернуто увагу науковцями [7, с. 26-27].

На нашу думку, характеризуючи стан справ у питанні розробки правових основ забезпечення кібербезпеки, слід звернути увагу на низку системних вад, що не береться до уваги при розробці фундаментальних документів стратегічного характеру.

По-перше, досить часто змішуються організаційні заходи, які можуть бути вирішені на рівні планування та впровадження державної політики або покращання ефективності виконання державними органами їх функціональних обов’язків, з правотворчою діяльністю, що викликає паралельну розробку нормативно-правових актів, які регламентують одне й те ж коло суспільних відносин у різних аспектах.

По-друге, при розробці законодавчих пропозицій поза увагою залишаються теоретичні питання, не в останню чергу питання розуміння правотворчої форми реалізації функцій держави, що проявляються у різних сферах людської діяльності. При цьому інформаційна сфера та сфера забезпечення кібербезпеки винятками у цьому не є.

Розглянемо, яким чином функції держави реалізуються у правотворчій формі в сфері регламентації кібербезпеки. Правотворча форма здійснення функції держави полягає у розробці, ухваленні та виданні нормативно-правових актів. Перелік функцій держави є предметом наукових дискусій і дослідити їх усі на рівні наукової статті не видається за можливе. Разом із цим вважається за доцільне дослідити ті функції держави, що є найбільш актуальними у сучасних умовах. До них слід віднести функцію оборони та функцію забезпечення державної безпеки.

Слід погодитись з висловленою у літературі точкою зору, що функція оборони держави полягає у цілеспрямованій діяльності держави щодо гарантування військової безпеки, цілісності території держави та непорушності кордонів шляхом застосування засобів військового характеру [15, с. 9]. На цей час застосування засобів військового характеру чинним законодавством прямо пов’язане зі станом війни. Проте гібридний характер сучасних війн, що зумовив появу неоголошених та невизнаних війн “де-факто”, вимагає перегляду підходів і у питанні правової регламентації застосування засобів військового характеру, що відомі як “кіберзброя”, застосування до суспільних відносин права війни та правових механізмів контролю за озброєнням [16, с. 54].

Безумовним є те, що функція забезпечення державної безпеки тісно пов’язана з функцією оборони, проте, водночас, вона має і свою специфіку. По-перше, загрози, що посягають на державний суверенітет, конституційний лад та територіальну цілісність держави, далеко не завжди є загрозами військового (збройного) характеру і не завжди виходять від інших держав-противників. По-друге, гібридність сучасних війн зумовлює і значне розширення суб’єктів військових дій, а також засобів, які ними обираються [17, с. 168-170; 18, с. 90]. За таких умов засоби та напрями державної політики, а також правової регламентації відрізняються від тих, що застосовуються при реалізації функції оборони держави.

На сьогодні можна стверджувати, що існує певна система законодавства, яке регламентує коло суспільних відносин, пов’язаних із реалізацією функції забезпечення державної безпеки. До цієї системи слід віднести законодавчі акти системного характеру, що ґрунтуються на положеннях Конституції України, законодавчі акти, що

визначають правовий статус окремих суб’єктів а також ті, що регламентують певну діяльність суб’єктів. Разом з цим суспільні відносини в інших сферах діяльності (насамперед в економічній) також перебувають під впливом правової регламентації відносин із забезпечення державної безпеки.

Таким чином, регламентація питання забезпечення державної безпеки у контексті вжиття заходів із кібербезпеки, повинна бути тісно пов’язана із правовою регламентацію компетенції відповідних державних органів. На жаль, розроблені останнім часом на виконання стратегічних настанов законодавчі пропозиції так і не дають відповіді на питання щодо визначення центрального органу виконавчої влади, який відповідає за проведення державної політики у сфері кібербезпеки. Далеко не у повному обсязі розробляється питання щодо регламентації відповідних повноважень державних органів, врахування при цьому прав і свобод людини і громадянина, особливостей захисту та відновлення порушених прав, дотримання при цьому вимог міжнародно-правових актів.

Слід зазначити, що повноваження з координації діяльності не повинні підміняти собою повноваження з реалізації державної політики у цій сфері. Практика європейських держав з цього приводу зводиться, як правило, до визначення (створення) уповноваженого державного органу виконавчої влади і наділення його відповідними повноваженнями. Наприклад, з прийняттям у липні 2015 року в Німеччині Закону “Про підвищення безпеки інформаційно-телекомунікаційних систем” (відомий як IT-Sicherheitsgesetz) розширені повноваження федерального відомства інформаційної безпеки (Bundesamt für Sicherheit in der Informationstechnik, BSI), у складі якого перебуває Національний центр кіберзахисту (Nationale Cyber-Abwehrzentrum (NCAZ). При цьому BSI, як федеральний орган, що знаходиться в підпорядкуванні МВС Німеччини, чітко наділений функціями і повноваженнями необхідними для їх виконання. Зазначена практика є досить розповсюдженою в європейських країнах (наприклад, Центр суспільної безпеки (NBU) Чехії має у своєму складі Суспільний центр кібербезпеки (NCKB) і є єдиним органом, що відповідає за державну політику в сфері кібербезпеки).

На жаль, в Україні інша ситуація. Як показує аналіз положень Стратегії кібербезпеки України, суб’єктами її забезпечення є мінімум 7 державних органів різного рівня, у тому числі підпорядкованих один одному. При цьому, під терміном “розвідувальні органи” згідно чинного законодавства може розумітись від 1 до 3 органів. Над усією цією системою з метою координації створено ще один орган – Національний координаційний центр кібербезпеки, до функцій якого згідно Положення про нього, затвердженого Указом Президента України від 07.06.16 р. № 242/2016, віднесено не тільки координуючі. При цьому, Державна служба спеціального зв’язку України (в структурі якої перебуває орган з функціями ідентичними німецькому NCAZ) є центральним органом виконавчої влади зі спеціальним статусом і не наділена функціями формування державної політики у сфері кібербезпеки, оскільки це суперечить положенням частини 2 статті 1 Закону України “Про центральні органи виконавчої влади”. Таким чином, слід констатувати, що формування державної політики з забезпечення кібербезпеки на жоден державний орган не покладено. Підготовлений проект законодавчого акту (проект Закону України “Про основні засади забезпечення кібербезпеки України”, який було прийнято Верховною Радою України за основу 20.09.16 р.) також оминає врегулювання цього питання.

На нашу думку, вирішення проблеми визначення статусу, функцій та наділення повноваженнями державного органу з формування та реалізації державної політики у сфері забезпечення кібербезпеки є основою для належної реалізації функцій оборони та забезпечення державної безпеки у сфері кібербезпеки.

Висновки.

1. Документи стратегічного планування у сфері забезпечення кібербезпеки визначають наявність низки загроз та викликів, встановлюють основні напрями державної політики у цій сфері, планують проведення організаційних заходів. Водночас, у питанні розробки нормативно-правових актів відсутній системний підхід та належне теоретичне підґрунтя.

2. На нашу думку доречним є сприйняття при законотворчості теоретико-правових конструкцій щодо розуміння правотворчої форми реалізації окремих функцій сучасної держави, насамперед, враховуючи умови гібридної війни проти України, мова йде про функцію оборони і забезпечення державної безпеки.

3. Основою для реалізації зазначених функцій держави має бути визначення статусу, функцій та наділення повноваженнями державного органу з формування та реалізації державної політики у сфері забезпечення кібербезпеки.

Використана література

1. Недільніченко В.Д. Розвиток інформаційних технологій і національна безпека України // Національна безпека : український вимір. – 2009. – № 3 (22). – С. 43-57.

2. Дубов Д.В. Кібербезпека: світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : НІСД, 2011. – 30 с.

3. Словник термінів з кібербезпеки ; уклад. Бутузов В.М., Гавловський В.Д., Довгань О.Д. [та ін.] ; за заг. ред. Копана О.В., Скулиша Є.Д. – К. : ВБ “Аванпост-Прим”, 2012.

4. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека : сутність, визначення, відмінності // Інформація і право. – 2012. – № 2. – С. 162-169.

5. Петров В.В. Щодо формування національної системи кібербезпеки України // Стратегічні пріоритети. – 2013. – № 4 (29). – С. 127-130.

6. Баранов О.А. Про тлумачення та визначення поняття “кібербезпека” // Правова інформатика. – 2014. – № 2(42). – С.54-62.

7. Пилипчук В.Г. Забезпечення інформаційної безпеки України : сучасні тенденції та проблеми : матеріали наук.-практ. конф. [“Запобігання новим викликам та загрозам інформаційній безпеці України: правові аспекти”], (Київ, 6 жовтня 2016 р.) / НТУУ “КПІ імені Ігоря Сікорського” ; упоряд. В.М. Фурашев. – К. : Вид-во “Політехніка”, 2016. – С. 24-28.

8. Грищук Р.В. Інформаційна та кібернетична безпека : роль та місце в умовах гібридної війни : матеріали всеукр. наук.- практ. конф. [“Кібербезпека в Україні : правові та організаційні питання”], (Одеса, 21 жовтня 2016 р.). – Одеса : ОДУВС, 2016. – С. 15-16.

9. Архипов А. Приставка кибер- : все ли очевидно? // Захист інформації. – 2016. – Т. 18. – № 3. – С. 203-209.

10. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. – 2014. – № 1(2) – С. 22-27.

11. Dunlop Charles. Perspectives for Cyber Strategists on Law for Cyberwar / Charles J. Dunlop // Strategis Studies. – 2011. – Spring Issue. – P. 81-99.

12. Finnemore M. Constructing Norms for Clobal Cybersecurity / M Finnemore, D. Hollis // American Journal Of International Law. – 2016. – Vol. 110[425] – P. 425-479.

13. Sabillon R. National Cyber Security Strategies : Global Trends in Cyberspace / R.Sabillon, V.Cavaller, J. Cano // International Journal Of Computer Science and Software Engineering. – 2016. – Vol. 5, Issue 5 – P. 67-80.

14. О кибербезопасности критической инфраструктуры государства / [М.А. Шнепс-Шнеппе, С.П. Селезнев, Д.Е. Намиот, В.П. Куприяновский] // International Journal of Open Information Technologies. – 2016. – Vol. 4. – № 7 – P. 22-31.

15. Волинець В. Правові аспекти реалізації оборонної функції сучасної держави // Юридична Україна. – 2013. – № 5. – С. 4-10.

16. Ford Christopher. The Trouble with Cyber Arms Control / Christopher A. Ford // The New Atlantis. – 2010. – № 29. – P. 52-67.

17. Chaudhry Rajeev. Violent Non-State Actors ; Contours, Challenges and Consequences / R.Chaudhry // CLAWS Journal. – 2013. – Winter Issue. – P. 167-187.

18. Mulford Joshua. Non-State Actors in the Russo-Ukrainian War / Joshua P. Mulford // Connections : The Quarterly Journal. – 2016. – № 2. – P. 89-107.

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

УДК 343.1

КОВАЛЬОВ К.Є., старший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ
ЛЕОНОВ Б.Д., *доктор юридичних наук, старший науковий співробітник,* провідний науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБУ

ЗАБЕЗПЕЧЕННЯ ОХОРОНИ ДЕРЖАВНОЇ ТА СЛУЖБОВОЇ ТАЄМНИЦІ У СФЕРІ ОПЕРАТИВНО-РОЗШУКОВОЇ ДІЯЛЬНОСТІ ЗА ЗАКОНОДАВСТВОМ ОКРЕМИХ ДЕРЖАВ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Анотація. *У статті висвітлена організація охорони оперативно-розшукової інформації в окремих країнах світу.*
Ключові слова: *державна таємниця, оперативно-розшукова діяльність, світовий досвід, інформаційна безпека, законодавство.*

Аннотация. *В статье освещена организация охраны оперативно-розыскной информации в отдельных странах мира.*
Ключевые слова: *государственная тайна, оперативно-розыскная деятельность, мировой опыт, информационная безопасность, законодательство.*

Summary. *The organization of protection of operative and intelligent information in certain countries of the world is highlighted in this article.*
Keuwords: *the state secret, operative and intelligent activity, world experience, information security, legislation.*

Постановка проблеми. У Стратегії національної безпеки України, затвердженій Указом Президента України від 26.05.15 р. № 287 [1], зазначається, що одним із пріоритетів забезпечення кібербезпеки і безпеки інформаційних ресурсів є реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав – членів НАТО та ЄС. Водночас, у ст. 7 Закону України “Про основи національної безпеки України” [2] визначено загрози національній безпеці України в інформаційній сфері, однією з яких є розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю.

Одним із напрямів правоохоронної діяльності, яка захищена за допомогою інституту таємниць, є оперативно-розшукова діяльність, і це не є випадковістю. Адже держава завжди убезпечувала найбільш чутливі сторони свого існування саме за допомогою обмеження доступу до інформації про них. Тим більш, що в оперативно-розшуковій діяльності особливе місце займає принцип забезпечення конспірації її провадження.

Дослідженням проблем захисту інформації з обмеженим доступом займалися багато вчених, але в контексті охорони державної таємниці слід виділити роботи О.Є. Архіпова, Р.В. Корсуна, В.М. Лопатіна, В.В. Макаренка, І.М. Мейдича, А.С. Пашкова, О.В. Шамсутдінова та М.В. Шлапаченка.

Водночас, охорона державної таємниці потребує удосконалення. Зростає також і роль порівняльного кримінального права. Бажано дослідити проблему охорони інформації з обмеженим доступом і під цим кутом зору.

Метою статті є порівняльний аналіз охорони державної та службової таємниці за законодавством окремих держав для удосконалення законодавства України у цій сфері.

Виклад основного матеріалу. Французький компаративіст Рене Давид, розглядаючи право різних країн, виділяє три основні групи правових систем: романо-германську правову сім’ю, сім’ю загального права і сім’ю соціалістичного права [3, с. 40].

Для порівняння достатньо розглянути відповідне законодавство кількох країн – репрезентантів правових систем, що належать до згаданих сімей права. Перш за все, це законодавство ФРН, (романо-германська правова сім’я), Англії та США (сім’я загального права).

У Німеччині система захисту державних секретів перетинається із загальною системою захисту значущих секретів у сфері промисловості й торгівлі (промислове шпигунство) та регулюється нормами низки законів, до яких відносяться: Кримінальний кодекс, Закон про боротьбу з недобросовісною конкуренцією, Постанова про боротьбу з підкупом не посадових осіб, Федеральний закон про охорону даних тощо. Кримінальний кодекс Німеччини, наприклад, містить положення про те, що державною таємницею є факти, об’єкти й інформація, доступні лише обмеженому колу осіб, які повинні зберігатися в секреті від іноземних держав з метою недопущення спричинення шкоди зовнішній безпеці Федеративної республіки.

Удосконалення захисту державних секретів здійснюється за трьома напрямами: вдосконалення законодавства у сфері захисту державних секретів і секретів фірм; посилення органів контррозвідки та надання їм великих повноважень, у тому числі й у сфері захисту державних секретів; створення організацій “самодопомоги” в промисловості та розгортання їх діяльності.

Важливим у вдосконаленні захисту секретів під час проведення науково-дослідних робіт військового призначення в Німеччині є посилення повноважень органів контррозвідки, і, зокрема, тих її підрозділів, які здійснюють боротьбу зі шпигунством і опікуються захистом державних секретів, у тому числі й у промисловості.

У системі забезпечення захисту державних секретів у питаннях боротьби з “промисловим шпигунством” іноземних держав важлива роль відводиться об’єднанням промисловців, так званим організаціям “самодопомоги”.

До таких організацій відноситься, наприклад, “Координаційний центр по забезпеченню безпеки в промисловості”, створений у Кельні в 1969 році, який вирішує проблеми забезпечення режиму секретності в промисловості держави [11].

У ФРН інформація з обмеженим доступом може мати три ступені секретності: “цілком таємно” (Streng Geheim); “таємно” (Geheim); “конфіденційно” (VS-Vertraulich). Слід зазначити, що у ФРН до державної таємниці відносяться лише відомості, які необхідно зберігати в секреті від іноземних держав з метою недопущення завдання шкоди зовнішній безпеці Федеративної республіки. В той же час відомості, які містять інформацію про проведення оперативно-розшукових заходів, належать до службової таємниці та охороняються відповідним законодавством. Відповідальність за порушення службової таємниці встановлена у 28 розділі Кримінального кодексу ФРН. Відповідні документи, що містять службову таємницю, позначають грифом “Для службового користування” (VS nur fur den dienstgebrauch).

Якщо документи для службового користування обробляються в автоматизованих системах, то мають бути дотримані певні вимоги безпеки. А саме автоматизовану систему має бути обладнано фаєрволом, у випадку підключення до мережі Інтернет, має бути затверджений перелік осіб, які мають доступ до автоматизованої системи,

використовуватися механізми автентифікації та ідентифікації (ім’я користувача та пароль), обов’язковою є наявність Інструкції з ІТ-безпеки тощо [12, Section II (1)].

Основним джерелом кримінального права ФРН є Кримінальний кодекс, що був прийнятий 15 травня 1871 р., і діє в редакції від 13 листопада 1998 р.

Розділ 2 Особливої частини КК ФРН має назву “Зрада батьківщині та загроза зовнішній безпеці”. Ця глава складається з 13 статей, в яких, зокрема, містяться норми про відповідальність за розголошення державної таємниці (§ 95), зрадницьке або інше вивідування державної таємниці (§ 96), видачу державної таємниці (§ 97), видачу нелегальної таємниці (§ 97-a), розголошення відомостей, помилково прийнятих за державну таємницю (§ 97-b).

Відповідно до абз. 1 § 95 КК ФРН під “розголошенням державної таємниці” розуміється створення неправомочній особі доступу або публічне оголошення охоронюваної державної таємниці, що створює загрозу спричинення тяжкої шкоди зовнішній безпеці Федеративної Республіки [13].

“Неправомочною” визнається будь-яка особа, яка за родом служби чи роботи не має права володіти даними відомостями. Цією особою може буде також визнаний іноземний громадянин, якщо він не відповідає ознакам спеціального адресата (§ 94 КК ФРН), тобто не належить до іноземної розвідки чи іноземного уряду. Слід зазначити, що застосування цієї норми обмежується тими випадками, коли у винного відсутній конспіративний зв’язок із представником іноземного уряду або зрадницький умисел, інакше таке діяння кваліфікується як шпигунство (§ 94 КК ФРН).

Під публічним розголошенням розуміють особливий випадок повідомлення державної таємниці неправомочним особам, коли винний своїми діями робить таку інформацію відомою відразу великій кількості осіб.

Для притягнення до кримінальної відповідальності необхідно, щоб винний усвідомлював, що відомості, які розголошуються, є державною таємницею і що вони повідомляються неправомочній особі. Якщо ця умова відсутня, то особа до кримінальної відповідальності не притягується за відсутністю складу злочину. Необхідною умовою є також розуміння винним того, що відомості передаються саме сторонній особі, а не представникові іноземної держави. Це відповідає пануючому у німецькій доктрині визначенню умислу, сформульованому Верховним Судом ФРН: “Умисел – це воля до здійснення складу злочину при усвідомленні всіх його обставин” [14, с. 212].

Особливістю даної кримінально-правової норми є те, що законодавець не пов’язує відповідальність зі спеціальним суб’єктом. Таким чином, у § 95 КК не проводиться різниці між особами, яким відомості, що становлять державну таємницю, були довірені по службі чи роботі, і приватними особами. Це, на нашу думку, слабкий бік німецького законодавства, яке невиправдано розширює сферу кримінальної репресії за розголошення державної таємниці.

Санкція § 95 КК передбачає покарання у виді позбавлення волі на строк від 6 місяців до 5 років. За наявності обтяжуючих обставин строк зазначеного покарання зростає до 10 років. Таким чином, позбавлення волі є, в даному випадку, єдиним безальтернативним видом покарання.

У разі необережного розголошення державної таємниці дії винного кваліфікуються за § 97 КК ФРН, що має назву “Видача державної таємниці”. В абз. 1 § 97 цього Кодексу йдеться про поєднання умисного розголошення державної таємниці з необережним створенням загрози заподіяння шкоди зовнішній безпеці країни. Розголошуючи державну таємницю, особа повинна діяти умисно, тобто усвідомлювати факт розголошення й характер відомостей, що розголошуються. Щодо

наслідків розголошення її вина полягає в необережності: особа не передбачає можливості настання тяжкої шкоди для зовнішньої безпеки ФРН. Отже, можна дійти висновку, що названий злочин характеризується складною формою вини. Ця форма вини знайшла законодавче відображення в абз. 9 § 11 і сформульована так: “умисним є також діяння, що створює передбачений законом склад злочину, який щодо діяння передбачає умисел, а щодо спричиненого цим діянням спеціального наслідку вважає достатньою необережність” [12 с. 208].

Особа, яка вчинює такий злочин, передбачений абз. 1 § 97 КК, карається штрафом або позбавленням волі на строк до 5 років.

Абз. 2 § 97 КК ФРН встановлює відповідальність осіб, яким державна таємниця була довірена по службі, роботі чи за спеціальним розпорядженням відповідного державного органу [12 с. 208].

Виходячи зі змісту цієї норми, дії винного полягають у тому, що він “легковажно” робить надбанням неправомочної особи відомості, що становлять державну таємницю. Суспільна небезпечність такого злочину виражається в загрозі заподіяння тяжкої шкоди зовнішній безпеці республіки. Санкція цієї норми передбачає покарання у виді штрафу або позбавлення волі на строк до трьох років.

Якщо ж особа, яка має доступ до державної таємниці, одержує секретну інформацію від інших осіб, але не забезпечує її належної охорони, то § 97 КК ФРН не застосовується.

Особи, які вчинили діяння, передбачені § 97 КК ФРН, притягаються до кримінальної відповідальності тільки за вимогою федерального уряду, причому уряд має обґрунтувати необхідність покарання цієї особи. Як правило, потрібно встановити та вказати вид і розмір заподіяної шкоди зовнішній безпеці ФРН.

У Великій Британії існує закон з охорони державної таємниці, який має назву “Про державну таємницю” (Official Secrets Act). Цей Закон був прийнятий у 1989 р. Однак, історія законодавства з охорони державної таємниці у Великобританії сягає своїми коренями у далеке минуле. Вона бере початок з 1889 р, коли було вперше прийнято закон з аналогічною назвою.

Систему охорони державної таємниці викладено в настанові з охорони державної таємниці (Manual of Protective Security), на базі якої міністерства розробляють власні настанови.

Згідно з чинним законодавством Великобританії інформація з обмеженим доступом може мати чотири ступені секретності: “цілком таємно” (Top Secret); “таємно” (Secret); “конфіденційно” (Confidential); “для службового користування” (Restricted).

До інформації зі ступенем “цілком таємно” відносяться відомості, несанкціоноване розголошення яких може створити загрозу внутрішній стабільності Об’єднаного Королівства або дружніх йому країн; призвести до значних людських жертв; може завдати значної шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; заподіяти значну шкоду взаєминам з дружніми урядами або спричинити довгострокові збитки економіці Королівства.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей, є перелік потенційних мішеней терористів, база даних інформаторів та кримінальної розвідки тощо.

До інформації зі ступенем “таємно” відносяться відомості, несанкціоноване розголошення яких може обернутися підвищенням рівня міжнародної напруженості; серйозно зашкодити відносинам з дружніми урядами; безпосередньо загрожувати життю або завдати значної шкоди громадському порядку або безпеці та свободам особистості; завдати значної шкоди ефективності або безпеці британських чи

союзницьких сил або розвідувальним операціям; спричинити істотну матеріальну шкоду національним фінансам чи економіці та комерційним інтересам.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, є об’єкти спеціальних операцій; інформація, яка розшифровує особу інформатора, оскільки її розголошення може загрожувати його життю.

До інформації зі ступенем “конфіденційно” відносяться відомості, несанкціоноване розголошення яких може завдати матеріальної шкоди дипломатичним стосункам, що матиме наслідком офіційний протест або інші санкції; заподіяти шкоду безпеці та свободам особистості; завдати шкоди ефективності або безпеці британських чи союзницьких сил або розвідувальним операціям; спричинити шкоду національним фінансам чи економіці та комерційним інтересам; істотно підірвати фінансову спроможність основних (великих) організацій; перешкодити розслідуванню або полегшити вчинення тяжкого злочину тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, є відомості про інформаторів, які не розкривають їх справжньої особи, проте розголошення яких може загрожувати безпеці інформаторів; відомості про спеціальні операції, розкриття яких може зашкодити розслідуванню тяжких злочинів; відомості про характер злочинної діяльності та можливі методи її припинення.

До інформації зі ступенем “для службового користування” відносяться відомості, несанкціоноване розголошення яких може зашкодити міжнародним стосункам, ускладнити забезпечення ефективності або безпеки британських чи союзницьких сил; завдати шкоди розслідуванню або полегшити скоєння злочину; завдати фінансової шкоди фізичним або юридичним особам, ускладнити управління державним сектором тощо.

Прикладом правоохоронної інформації, яка відноситься до цієї категорії відомостей у Великій Британії, може бути інформація, отримана від поліції іншої країни, якщо така інформація не була загальновідомою, покази (свідчення) осіб у справі, розголошення яких може зашкодити розслідуванню тощо.

Існуюча в Англії система захисту державних секретів базується на Законі “Про державну таємницю” (Official Secrets Act), що був розроблений у 1988 р., а набув чинності з 1 березня 1990 р. Цей законодавчий акт замінив раніше діючий закон про державну таємницю, прийнятий ще в 1911 р.

У новому законі конкретизовані формулювання складів злочинів, пов’язаних із розголошенням інформації, що охороняється, більш чітко подане визначення відомостей, які становлять державну таємницю, уточнені поняття збитків, що завдаються державі внаслідок розголошення тих чи інших відомостей.

Чинне кримінальне законодавство Англії розрізняє випадки розголошення державної таємниці особами, які володіють нею за своїм службовим становищем, а також особами, які не мають прямого доступу до такої таємниці.

Перші чотири статті нового закону про державну таємницю передбачають відповідальність спеціального суб’єкта (державного службовця чи підрядчика державної установи) за вчинення злочину, що розглядається. Першочергового значення набувають кримінально-правові заходи, спрямовані на захист від розголошення відомостей про всі аспекти діяльності розвідувальних і контррозвідувальних органів Великобританії.

Злочином вважається розголошення співробітниками спецслужб (у тому числі й колишніми) будь-яких відомостей про їх діяльність. Mens rea (“винна воля”) даного злочину полягає лише у намірі вчинити заборонені законом дії, оскільки для настання відповідальності за передачу секретної інформації не має значення факт спричинення шкоди безпеці та інтересам держави. Отже, владі немає потреби доводити наявність

шкоди чи збитків, завданих таким розголошенням. До кримінальної відповідальності притягується й технічний персонал спецслужб, а також службовці організацій, що виконують замовлення спецслужб, якщо вони розголошують інформацію, отриману в результаті виконання своїх обов’язків. Лише одна обставина при цьому звільняє від відповідальності – незнання, що розголошена інформація стосується діяльності спецслужб і її розголос може завдати шкоди їх діяльності (ст. 1) [15, с. 188].

З цих же підстав притягається до відповідальності особа, яка маючи у своєму розпорядженні або під своїм контролем секретні шифр, пароль, предмет, запис та інші документи, отримані у порушення законів про державні секрети або в результаті доступу до них, пов’язаного з її посадою, передала зазначені секретні матеріали тому, хто не уповноважений їх отримувати.

Розголошення відомостей щодо оборони або міжнародних відносин переслідується в кримінальному порядку, однак обвинувач (держава в особі органів прокуратури) повинен довести наявність реальних збитків (статті 2 і 3). Наприклад, при розгляді справи про розголошення інформації щодо національної оборони обвинувач зобов’язаний навести конкретні факти ослаблення бойової могутності збройних сил.

Злочином вважається також розголошення інформації, яка може бути використана злочинцями, якщо в результаті цієї дії виникає чи може виникнути будь-який з наступних наслідків: здійснюється злочин чи втеча з-під варти, ускладнюється запобігання вчиненню злочинів чи їх розслідування, виникають перешкоди в затримці чи кримінальному переслідуванні злочинців (ст. 4).

У законі встановлена кримінальна відповідальність і за дії, що сприяють розголошенню секретної інформації: недбале зберігання документів і розголошення відомостей, які полегшують несанкціонований доступ до державної таємниці, а також порушення офіційних розпоряджень, що регламентують зберігання та роботу із секретними документами (ст. 8). До кримінальної відповідальності можуть притягатися також особи, які не є державними службовцями чи підрядчиками державних установ. Насамперед це стосується працівників засобів масової інформації, зокрема журналістів, які різними шляхами прагнуть отримати секретну інформацію. Щоб домогтися засудження, сторона обвинувачення має довести, що в особи були достатні підстави вважати, що розголошена нею інформація захищена законом і що її розголошення завдасть шкоди національним інтересам країни (ст. 5). Тобто для судового переслідування необхідна наявність mens rea – прямого умислу [15, с. 388].

У законі також передбачена кримінальна відповідальність за несанкціоноване розголошення секретної інформації, якщо вона раніше була передана урядом Великобританії іншій державі чи міжнародній організації та була вперше розголошена за кордоном (ст. 6). Сторона обвинувачення має довести, що розголошена (найчастіше у журналістській публікації) інформація є державною таємницею, а її витік завдав чи міг завдати шкоди. Крім того, тут теж необхідно спиратися на наявність mens rea: обвинувачуваний повинен був знати про характер інформації, що ним розголошується, та про можливу шкоду. Недоведеність будь-якого з перерахованих фактів призводить до виправдання обвинуваченого.

Обставинами, що звільняють від кримінальної відповідальності, не можуть бути твердження обвинуваченого, що розголошення інформації не може завдати шкоди, оскільки вона вже опублікована за кордоном [14, с. 190].

Отже, при розголошенні державної таємниці сторона обвинувачення в більшості випадків має доводити наявність шкоди, завданої цим розголошенням, причому з різними категоріями інформації пов’язані різні категорії шкоди.

За розголошення відомостей, що становлять державну таємницю, передбачається покарання у вигляді тюремного ув’язнення строком до 2 років, штрафу до 2 тис. фунтів стерлінгів чи два покарання одночасно. За вчинення дій, що сприяють такому розголошенню, винний карається позбавленням волі строком до 3 місяців, штрафом до 2 тис. фунтів стерлінгів чи двома покараннями (ст. 10).

Кабінет міністрів Великобританії вживає активних заходів щодо запобігання витоку секретних відомостей через засоби масової інформації, керуючись при цьому положеннями закону про державну таємницю, а також адміністративного закону про конфіденційність. Відповідно до положень останнього уряд має право вимагати через суд першої інстанції заборони публікації певних матеріалів шляхом внесення окремої ухвали судді без зазначення осіб, щодо яких застосовується заборона. Внаслідок цього автору і видавцям можуть заборонити публікування матеріалів за кордоном. Суд має право зобов’язати ініціаторів публікації забрати рукопис з будь-якого іноземного видавництва. Уряд може вимагати від видавців і автора подати на розгляд зміст публікації і перелік використаних джерел, якщо вони бажають, аби заборона була знята.

У США система обмеження доступу до певних відомостей регулюється Указом Президента “Секретна інформація в сфері національної безпеки”, відповідно до якого в США існують три ступені секретності: “цілком таємно” (Top Secret), “таємно” (Secret) та “конфіденційно” (Confidential).

Причому, до інформації зі ступенем секретності “цілком таємно” відносяться відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, до інформації зі ступенем секретності “таємно” – відомості, несанкціоноване розкриття яких може завдати значної шкоди національній безпеці, а до інформації зі ступенем секретності “конфіденційно” – відомості, несанкціоноване розкриття яких може завдати шкоди національній безпеці (Section 1.2 [16]).

До категорій інформації, яка може бути засекречена, відносяться відомості про військові плани, озброєння або операції; інформація іноземних урядів; відомості про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи або криптологію; іноземні відносини або закордонні заходи США, включаючи конфіденційні джерела; наукову, технологічну або економічну діяльність щодо забезпечення національної безпеки, яка забезпечує захист від міжнародного тероризму; програми США щодо безпеки ядерних матеріалів та обладнання; вразливості та можливості систем, установок, інфраструктур, проектів, планів або захисних служб національної безпеки, які забезпечують захист від міжнародного тероризму або зброї масового знищення.

Інші категорії інформації засекречувати забороняється.

Відповідно до згаданого Указу Президента США державні органи розробляють власні інструкції щодо роботи з державною таємницею.

Як правило, окремі відомості щодо проведення оперативно-розшукових заходів відносять до державної таємниці на підставі їх належності до відомостей про розвідувальні заходи (включаючи спеціальні заходи), розвідувальні джерела чи методи отримання розвідувальної інформації.

При розгляді в суді кримінальних справ може виникнути необхідність у розкритті окремих секретних аспектів оперативно-розшукової діяльності. В такому разі суди США користуються Законом “Про процедури з секретною інформацію” (Classified Information Procedures Act) (18 U.S.C. App. IV) 1980 р. Відповідно до цього закону в разі, якщо суддя вважатиме, що розкриття секретних відомостей є необхідним для вирішення питання про невинність підсудного, він має право вимагати розкриття таких відомостей.

Якщо в розкритті таких відомостей буде відмовлено відповідним державним органом, то судове переслідування припиняється. Як показує судова практика, в більшості випадків, коли виникали подібні ситуації, судове переслідування припинялося.

Крім цього, в даному контексті слід також відзначити Указ Президента США “Про структурну реформу щодо підтримання безпеки секретних мереж та обґрунтованого поширення та убезпечення секретної інформації” (Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information) від 07.10.11 р. № 13587, який присвячено захисту секретної інформації, що циркулює в комп’ютерних мережах.

Кримінальне право США, яке запозичило положення англійського кримінального права, відрізняється своєрідністю. Норми кримінально-правового характеру зібрані головним чином у розділі 18 Зводу законів США, реформованого ще в 1948 р. (це так званий Федеральний кримінальний кодекс США) [17]. В окремих штатах діють свої кодекси: КК штату Нью-Йорк 1965 р., що являє собою главу 40 Зводу законів цього штату, КК Аляски 1978 р. тощо.

У США немає єдиного підходу до законодавчого встановлення кримінально-правової охорони державних секретів. В структурі правових джерел і в класифікації норм федерального законодавства та окремих штатів спостерігається помітне розмаїття.

З одного боку, діє закон про покарання за розголошення офіційної інформації (1985), який за дане діяння передбачає покарання у вигляді штрафу в розмірі 15 тис. доларів чи трьох років тюремного ув’язнення, або обидва види покарання одночасно. З іншого боку, існує директива міністерства оборони США “Про нерозголошення важливої технічної інформації” (1984 р.), відповідно до якої винному загрожує тюремне ув’язнення або штраф – 1 млн. доларів чи на суму, що вп’ятеро перевищує вартість збитків, завданих розголошенням [18, с. 26].

Активно ведеться боротьба і з витоком офіційної інформації про діяльність американських розвідувальних служб, про їх співробітників і агентуру. Так, закон про захист особового складу розвідки (1982 р.) за розголошення зазначених відомостей передбачає штраф у розмірі до 50 тис. доларів чи тюремне ув’язнення строком до 10 років, або обидві міри покарання одночасно.

Крім зазначених нормативно-правових актів, норми федерального законодавства, що регулюють кримінальну відповідальність за злочини, пов’язані з розголошенням офіційної інформації, містяться також у розділі 18 Зводу законів США (“Кримінальне право та процес”), у розділі 50 (“Війна і національна безпека”) та в інших розділах Зводу законів. Ці норми відрізняються надзвичайною казуїстичністю, особливо при перерахуванні секретних об’єктів або способів злочинних посягань на державну таємницю.

Так, федеральний Звід законів у § 793 передбачає кримінальну відповідальність за умисне повідомлення, передачу, надіслання матеріалів чи інформації щодо національної оборони “якій-небудь особі, не уповноваженій на її одержання”, або спробу чи сприяння вчиненню таких дій, якщо особа “має підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане на користь іноземній державі” [19, с. 40].

Для цього складу злочину характерним є спеціальний суб’єкт: особа, яка на законних підставах має доступ, контролює чи володіє довіреними їй відповідними матеріалами чи інформацією.

Для притягнення до кримінальної відповідальності за розголошення інформації щодо національної оборони, намір завдати шкоди не потрібний. Достатньо того, що обвинувачений усвідомлював важливість інформації, оскільки в даному випадку, як заявив

юридичний комітет Сенату, “йдеться про профілактичні заходи, щоб секретний матеріал не міг потрапити до ворога, а не про боротьбу з активним шпигунством” [20, с. 224].

Крім того, у федеральному законодавстві встановлена кримінальна відповідальність за необережне (“через грубу недбалість”) видалення з місць зберігання чи передачу будь-якій неуповноваженій особі зазначених у § 793 d матеріалів чи інформації або неповідомлення вищестоящій посадовій особі про таке видалення чи передачу при вказаних вище суб’єктивних ознаках, тобто маючи підстави вважати, що це завдасть шкоди Сполученим Штатам чи стане у нагоді іноземній державі. Суб’єктом у даному випадку виступає як особа, якій довірена або котра володіє чи контролює таку інформацію, тобто спеціальний суб’єкт (§ 793 f Зводу законів США), так і особа, яка незаконно володіє, має доступ чи контролює інформацію оборонного характеру, тобто загальний суб’єкт (§ 793 e) Зводу законів США).

Кожне з названих діянь тягне за собою покарання у вигляді штрафу в розмірі до 10 тис. доларів чи тюремного ув’язнення на строк до 10 років, або обидва покарання одночасно.

Федеральне законодавство передбачає кримінальну відповідальність також за незаконне фотографування або зарисовку важливих оборонних об’єктів, за публікацію або продаж таких фотографій, малюнків тощо. Згідно з §§ 795-797 Зводу законів США порушники цих правил, незалежно від їх суб’єктивних намірів чи “підстав вважати”, можуть бути позбавлені волі на строк до 1 року або оштрафовані на 1 тис. доларів.

У федеральному законодавстві США встановлена також кримінальна відповідальність за розголошення службової необоронної інформації, про яку йшлося вище. Особливому захисту підлягають коди, шифри, криптографічні системи, різні апарати та пристрої, що використовуються для забезпечення секретності інформаційних зв’язків США чи інших держав. “Свідоме і добровільне” розкриття відповідних відомостей не уповноваженій на ознайомлення з ними особі, а також їх публікація чи будь-яке використання на шкоду інтересам США караються позбавленням волі на строк до 10 років чи штрафом (§ 796 Зводу законів США). Такому ж покаранню підлягає винна особа за публікацію або розкриття будь-якій особі кодів чи змісту дипломатичного листування (§ 952 Зводу законів США). Окремо регулюється охорона секретів, пов’язаних з дослідженнями в галузі атомної енергії (§§ 2271-2281 розділу 42 Зводу законів США).

Федеральне законодавство і КК штатів містять також загальні і спеціальні норми про різного роду зловживання службовим становищем і незаконне поширення та використання інформації. При цьому суб’єктами посадових злочинів можуть бути не тільки так звані публічні посадові особи, але й звичайні службовці та наймані робітники органів публічної адміністрації, публічних корпорацій і державних банків. Суб’єктами посадових злочинів можуть бути також і будь-які інші особи.

У главі 93 розділу 18 Зводу законів США особливу групу зловживань становить діяльність чиновників у сфері використання службової інформації.

Так, вчиняє злочин, передбачений § 1902, посадова особа, службовець чи будь-яка особа, яка діє від імені США, департаментів або представництв, якщо вона в силу свого службового становища чи посади, володіючи якою-небудь інформацією, що має значення для торгівлі США та ринкової діяльності, свідомо й неуповноважено передає її особі, яка відповідно до закону або посадової інструкції не повинна отримувати таку інформацію. Цей злочин карається штрафом до 10 тис. доларів або (і) позбавленням волі на строк до 10 років. До цієї ж групи посадових злочинів належить і поширення інформації щодо діяльності Корпорації фінансової реконструкції (§ 1904). За такий злочин передбачене покарання у вигляді штрафу до 10 тис. доларів або (і) позбавлення волі на строк до 5 років.

Крім зазначених вище випадків розголошення спеціальної інформації, глава 93 (§ 1905) містить норму про відповідальність за розголошення секретних відомостей загального характеру. Відповідно до цієї норми, якщо посадова особа чи службовець державних установ США, що за родом своєї служби володіє секретною інформацією, пов’язаною з проваджуваним розслідуванням, даними анкет або секретами торгівлі, управління, стилю роботи, даними про персонал, устаткування, статистичними даними, сумами чи джерелами доходів, прибутками чи витратами будь-якої особи, фірми, компанії, корпорації, неуповноважено опубліковує, розкриває, розголошує чи будь-яким іншим способом поширює таку інформацію, то вона карається штрафом у розмірі до 1000 дол. або позбавленням волі строком до 1 року. Особа, засуджена за вчинення цього злочину, повинна бути звільнена з посади чи з місця роботи.

Очевидно, що система нормативних актів США в галузі охорони секретної інформації надто розгалужена, складна і громіздка, що, однак, пояснюється особливостями системи загального права, до якої належить і американське право. У законодавстві США існує не одна, як в Україні, а досить велика кількість кримінально-правових норм, які передбачають відповідальність за розголошення державної таємниці. Причому критерієм диференціації даних норм виступає, насамперед, предмет злочину. Інакше кажучи, кожній категорії офіційної інформації відповідає окрема норма федерального кримінального законодавства. Автори вважають, що дані положення американського законодавства неприйнятні для вітчизняної правової системи, особливо, якщо враховувати, що санкції аналізованих кримінально-правових норм США, котрі передбачають винятково великі розміри покарань, практично ідентичні [21].

Висновки.

Незважаючи на різницю в правовому регулюванні захисту інформації, яка є державною таємницею у Великобританії, США, ФРН, інформація про проведення конкретних оперативно-розшукових заходів та залучення осіб до конфіденційного співробітництва має обмежений доступ за законодавством цих країн. Для зазначеної інформації передбачено особливий порядок отримання, обробки, зберігання, захисту та розсекречування. В законодавстві цих країн процедурні питання роботи з такою інформацією схожі.

На підставі аналізу законодавства Великобританії та США слід дійти висновку, що для сім’ї загального права (Великобританії та США) характерним є більш докладні приписи щодо віднесення тієї чи іншої правоохоронної інформації до державної таємниці. Дана обставина зумовлена прецедентом англо-саксонської системи права, яка тяжіє до конкретизації судових рішень (з питань охорони оперативно-розшукової інформації), що можуть бути прийняті в рамках тих чи інших суспільних відносин. Законодавчий захист державної таємниці в США близький до британського в плані диференціації відповідальності залежно від категорії розголошеної інформації. Подібність полягає також у тому, що суб’єктами розголошення державної таємниці можуть бути особи, які не мають доступу до таких відомостей, тобто так звані приватні особи. При цьому американське законодавство розмежовує умисне й необережне розголошення державної таємниці та розглядає їх у рамках окремих правових норм.

Кримінальне законодавство ФРН не пов’язує відповідальність за розголошення державної таємниці зі спеціальним суб’єктом.

Таким чином, вважаємо, що виявлені у результаті порівняння особливості законодавства досліджених країн можуть бути враховані під час удосконалення законодавства України у сфері охорони інформації з обмеженим доступом.

Використана література

1. Стратегія національної безпеки України : Указ Президента України від 26.05.15 р. № 287/2015 // Офіційний вісник України. – 2015. – № 43. – Ст. 1353.

2. Про основи національної безпеки України : Закон України від 19.06.03 р. // Офіційний вісник України. – 2003. – № 29. – Ст. 1433.

3. Давид Р. Основные правовые системы современности / Р. Давид. – М., 1988. – С. 40.

4. О государственной тайне : Федеральный закон РФ от 21.07.93 г. / Российская газета. – № 182. – 21.09.93 г.

5. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти : Постановление Правительства РФ от 03.11.94 г. № 1233 / Собрание законодательства РФ. – 2005. – № 30 (ч. II). – Ст. 3165.

6. Об утверждении перечня сведений конфиденциального характера : Указ Президента РФ от 06.03.97 г. № 188 / Собрание законодательства РФ. – 1997. – № 10. – Ст. 1127.

7. Перечень сведений, отнесенных к государственной тайне : Указ Президента РФ от 30.11.95 г. № 1203 / Российская газета. – № 246. – 27.12.95 г.

8. Комментарий к Уголовному кодексу Российской Федерации ; отв. ред. В.И. Радченко ; науч. ред. А.С. Михлин. – М. : Спарк, 1999. – 862 с.

9. Уголовный кодекс Российской Федерации : постатейный комментарий. – М. : Зерцало, Теис, 1997. – 792 с.

10. Шамсутдінов О.В. Відповідальність за розголошення державної таємниці за новим кримінальним законодавством України // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001. – № 2. – С. 22-26.

11. Executive Order 13526 Classified National Security Information, December 29, 2009. – Режим доступу : http://edocket.access.gpo.gov/2010/pdf/E931418.pdf

12. Instruction sheet on the Handling of Protectively Marked Information Classified VSNUR FÜR DEN DIENSTGEBRAUCH (RESTRICTED). – Режим доступу : https://www.bsi.bund.de/ SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/VSMerkblattEnglisch_pdf.pdf?__blob=publicationFile

13. Уголовный кодекс ФРГ. – М. : Изд-во “Зерцало”, 2001. – 208 с.

14. Хавронюк М.І. Кримінальне законодавство України та інших держав континентальної Європи : порівняльний аналіз, проблеми гармонізації / М.І. Хавронюк : монографія. – К. : Юрисконсульт, 2006. – 1048 с.

15. Лейленд П. Кримінальне право : злочин, покарання, судочинство. – (Англ. підхід) / П. Лейленд . – К. : Основи, 1996. – 207 с.

16. Кримінальне право України. Загальна частина ; за ред. М.І. Бажанова, В.В. Сташиса, В.Я. Тація. – К.-Харків : Юрінком Інтер-Право, 2002. – 416 с.

17. Federal Criminal Code and Rules as amended to February 1, 1991. – St. Paul., 1991. – P. 953-1044.

18. Бантишев О.Ф. Як довести, що ти – не шпигун? / Політика і час. – 1994. – № 8. – С. 24-28.

19. Уголовное право Соединенных Штатов Америки : сб. нормативных актов ; сост., отв. ред. И.Д. Козочкин. – М. : Изд-во Ун-та дружбы народов, 1986. – 160 с.

20. Никифоров Б.С. Современное американское уголовное право / Б.С. Никифоров, Ф.М. Решетников. – М. : Наука, 1990. – 256 с.

21. Леонов Б.Д. Особливості відповідальності за злочини у сфері охорони державної таємниці за кримінальним правом деяких зарубіжних держав : порівняльно-правова характеристика : навч. посібник / Б.Д. Леонов, О.В. Шамсутдінов. – К. : Наук.-вид. відділ НА СБУ, 2009 – 92 с.

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

УДК 35.746.1

СЕМЕНЮК О.Г., *кандидат юридичних наук,*
заступник начальника Управління Служби безпеки України

ЕВОЛЮЦІЯ НАУКОВИХ ПОГЛЯДІВ НА ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ З ОХОРОНИ ДЕРЖАВНОЇ ТАЄМНИЦІ

Анотація. *У статті висвітлюються історичні аспекти теоретичних розробок проблеми охорони державної таємниці у їх взаємозв’язку з вихідними положеннями нормативної бази та сформованою практикою; обґрунтовується необхідність комплексного дослідження цієї проблеми.*

Ключові слова: *історія дослідження, державна таємниця, інформаційне право, адміністративне право, національна безпека.*

Аннотация. *В статье рассматриваются исторические аспекты теоретических разработок проблемы охраны государственной тайны в их взаимосвязи с основными положениями нормативной базы и устоявшейся практикой; обосновывается необходимость комплексного исследования этой проблемы.*

Ключевые слова: *история исследования, государственная тайна, информационное право, административное право, национальная безопасность.*

Summary. *The article highlights the historical aspects of theoretical development of state secret security issues in their connection with the original provisions of the regulations and established practice; substantiates the necessity of a comprehensive study of the problem.*

Keywords: *history of research, state secret, information law, administrative law, national security.*

Постановка проблеми. У структурі наукового дослідження сформульовані проблеми виступають як конкретні завдання, що підлягають вирішенню. Необхідно зазначити, що успішне виконання названих завдань можливе лише в тому випадку, якщо конкретна наука має необхідні й достатні для цього можливості, які в наукознавстві прийнято іменувати передумовами теорії. “Передумови – попередня умова існування, виникнення, діяння і т. ін. чого-небудь” [1, с. 725], у нашому випадку – умова створення та розгляду комплексу заходів з охорони державної таємниці.

Будь-яке дослідження повинно бути органічно пов’язаним із передумовою досліджуваного питання, оскільки ніяке сучасне наукове або філософське дослідження не може бути абсолютно безпередумовним. З перших же кроків нової проблемної ситуації воно завжди орієнтоване на пошуки більш або менш певного рішення. У загальному випадку орієнтиром, який визначає цілком конкретні ходи в новій проблемній ситуації, є сукупність теоретичних положень, які на цей час є в науковому арсеналі [2, с. 30]. Цю ж обставину підкреслює М. Бунге, на думку якого “ніколи не бувало ніякого нового знання, яке не визначалося б знанням, що йому передувало” [3, с. 110].

Погоджуючись із наведеними твердженнями, зазначимо, що наука не створюється однією людиною. Потреби суспільства й соціальна практика породжують, формують і створюють наукову думку протягом тривалого проміжку часу. Тому, перш ніж досліджувати систему охорони державної таємниці, необхідно дослідити її передумови. “Спроба вирішити проблему без дослідження її передумов настільки ж наївна, як і згода з тим чи іншим твердженням без аналізу передбачуваного обґрунтування” [4, с. 31].

Проблеми формування та розвитку вітчизняної системи охорони державної таємниці були предметом дослідження багатьох вітчизняних учених, зокрема: В. Артемова, А. Гуза, О. Ботвінкіна, Д. Вєдєнєєва, В. Ворожка С. Князєва, О. Колєсніка, А. Марущака, О. Розвадовського, В. Сідака, О. Шамсутдінова, В. Шлапаченка та інших. Однак необхідність комплексного аналізу державної таємниці та заходів забезпечення її охорони з позиції кримінологічної науки зумовлює проведення відповідного аналізу історіографії розвитку не тільки її теоретичних передумов, а й вихідних положень нормативної бази та сформованої практики.

Метою статті є аналіз історії дослідження та еволюції наукових поглядів на забезпечення діяльності з охорони державної таємниці, нормативної бази та сформованої практики.

Виклад основного матеріалу. З виникненням такого інституту, як держава, почала поширюватися практика оголошення певних відомостей таємними, встановлення та закріплення у правових нормах відповідних правил щодо порядку її обігу, охорони та відповідальності за їх порушення. Проте теоретичне осмислення проблем забезпечення охорони державної таємниці бере свій початок від 40-х років середини XX століття.

Дж. Бернал у книзі “Наука в історії суспільства” зазначав, що поява наук міцно пов’язана з історичним розвитком суспільства, обумовлюється тими новими задачами, які суспільство повинно вирішувати в інтересах свого подальшого існування [5]. Тому немає нічого дивного, що саме в період Другої світової війни та в умовах тоталітарного політичного режиму в СРСР, який супроводжувався масовими порушеннями прав людини, охорона державної таємниці набуває гіпертрофованих форм і з’являється перша наукова праця М. Дурманова “Державна та військова таємниці”, у якій він обґрунтовував суспільну небезпеку порушень правил поводження з державною таємницею та намагався довести необхідність застосування жорсткого покарання за розголошення державної та військової таємниць, вбачаючи в цьому дієвість та необхідність заходів їх захисту [6].

Такий звужений підхід до проблеми охорони державних секретів пояснювався тим, що покарання за радянським кримінальним правом вважалося одним із необхідних засобів вирішення задачі скорочення, а згодом і повного викорінення злочинності в нашому суспільстві. Кінцевою метою кримінального покарання, як зазначав М. Бєляєв, є ліквідація злочинності [7, с. 20-21].

Радянське кримінальне законодавство мало своїм завданням захистити передусім державні інтереси, а розголошення державної таємниці розглядалося як посягання на державну безпеку. Тому процес криміналізації розголошення державної таємниці та його наукове обґрунтування характеризуються об’єктивними закономірностями розвитку суспільства, його зовнішньо- і внутрішньополітичною ситуацією, стійкими особливостями, зумовленими найбільш суттєвими, базисними тенденціями соціально-політичного характеру.

У радянську епоху державною безпекою СРСР визнавався стан непорушності “корінних основ розвинутого соціалістичного суспільства в умовах гострого класового протиборства сил соціалізму та імперіалізму” [8, с. 9]. Державна безпека була покликана створювати панівному класу умови для здійснення та зміцнення своєї політичної влади. При цьому державній таємниці, крім захисту державної безпеки, відводилася роль обмеження демократичних інститутів, посилення влади державного апарату. Для цього періоду характерним є процес тотального засекречування різних відомостей, які стосувалися діяльності органів державної влади.

Починаючи з 70-х років XX століття в адміністративній науці стала формуватися теорія адміністративно-правових режимів, єдиною метою яких вважалося забезпечення загальної безпеки в державі. Зокрема, І. Розанов зазначав, що загальною метою й основним призначенням адміністративно-правових режимів є створення на шляху іноземних розвідок, злочинних організацій і осіб надійних правових бар’єрів та розроблення організаційних заходів для забезпечення останніх, які б серйозно ускладнювали, а то й унеможливлювали досягнення злочинної мети у сфері зовнішньої і внутрішньої безпеки [9, с. 86].

Для охорони державної таємниці було запроваджено таке поняття, як спеціальний адміністративно-правовий режим секретності, який, як зазначав Д. Бахрах, з одного боку, є важливим засобом забезпечення державної безпеки, а з іншого, засекречування – це передбачене Конституцією обмеження закріпленого конституційного права громадян “вільно шукати, отримувати, виробляти та розповсюджувати інформацію в будь-який законний спосіб”. При цьому режим секретності є постійним та загальнодержавним, а до його головних елементів належать: 1) правила засекречування; 2) захист державної таємниці; 3) розсекречування [10, с. 214].

Незважаючи на те, що наведене визначення режиму секретності містить окремі суперечності, оскільки розсекречування не є засобом обмеження права на доступ до інформації, а навпаки знімає заборони щодо доступу до такої інформації, воно дозволило відійти від класичного розуміння охорони державної таємниці виключно за допомогою кримінального покарання.

Тривалий час дослідження державної таємниці в рамках адміністративного права повністю задовольняло потреби радянських науковців і пояснювалося тим, що ці відносини вписувалися в предмет цієї галузі права, суспільним призначенням якої вважалося, з одного боку, виконання функцій управлінського права, тобто засобу управлінського впливу держави на суспільні процеси, з іншого – як карального права, яке регламентує використання державою у відносинах із громадянами різноманітних засобів адміністративного впливу.

Сучасне українське адміністративне право вже не відповідає такому класичному призначенню, у зв’язку з чим його функція залишається істотно деформованою та вже не відповідає якісно новій демократичній моделі політичної системи європейського зразка, яка вимагає перегляду існуючих наукових позицій, законодавства, структури та діяльності державного апарату.

На жаль, традиційні стереотипи звичного ставлення до предмету адміністративного права дуже стійкі. На цьому тлі намітилася й отримала підтримку найбільш небезпечна тенденція – не змінювати, не переглядати докорінно свою діяльність, а лише вдосконалювати те, що робилося впродовж тривалого часу. Некритичне сприйняття запроваджених радянськими вченими штучно створених конструкцій, обумовлених цілями та задачами соціальної та політичної боротьби, які в інших країнах вже давно стали надбанням історії, понять та побудов, які змінювалися разом із політикою держави, призвело до того, що й донині при визначенні поняття адміністративно-правового режиму здебільшого наголошують на трьох аспектах: застосуванні адміністративно-правових засобів регулювання, наявності юридично нерівних позицій між учасниками певних відносин та наявності імперативного методу юридичного впливу [11, с. 325; 12, с. 38; 13, с. 268; 14, с. 91].

Теза щодо імперативного методу регулювання (здійснюється згори, тобто на владно-імперативній основі) порушує такий важливий загально-правовий принцип сучасного права, як рівноправність учасників правових відносин. Це обумовлює

необхідність відмови від розуміння забезпечення режиму секретності у якості встановленої в законодавчому порядку сукупності правил діяльності, дій або поведінки громадян, юридичних осіб, а також державних органів та їх посадових осіб, в основу яких покладено владно-управлінські повноваження.

Крім цього, при дослідженні питання щодо охорони державної таємниці слід враховувати ту обставину, що відносини, які виникають у цій сфері, вже давно вийшли за рамки суто адміністративних і регулюються різними галузями права. Так, можливість обмеження конституційних прав і свобод громадянина, зокрема щодо доступу до інформації, становить предмет конституційного права. Питання звільнення особи із займаної посади, якій скасовано допуск до державної таємниці, матеріальні компенсації за роботу з державною таємницею урегульовані трудовим законодавством. Відповідальність за порушення законодавства про державну таємницю регламентується нормами трудового, адміністративного та кримінального права. Контррозвідувальна діяльність та запобігання таким порушенням також виходять за межі адміністративного права.

Реально існуюча вузькість адміністративного права суттєво обмежує діапазон дослідження питань, які не відносяться до його предмета. Практика доводить, що при підході до дослідження проблем охорони державної таємниці з позицій і засобами адміністративного права названі проблеми якщо і вирішуються, то лише односторонньо, поверхнево й тому незадовільно. Тому подальша розробка проблем охорони державної таємниці в рамках цієї галузі буде здійснюватися на їх шкоду.

Після проголошення Україною в 1991 році незалежності та унормуванням на законодавчому рівні більшості питань щодо охорони інформації з обмеженим доступом, які до цього регулювалися засекреченими відомчими інструкціями, цією сферою відносин зацікавилися представники інформаційного права.

Слід зауважити, що вже в першому науковому дослідженні законодавчих актів України, які врегульовували інформаційні відносини, А. Письменицький наголошував на необхідності включення в предмет інформаційного права питання правового регулювання режиму інформації, у т.ч. і державної таємниці [15]. Проте аналіз наступних наукових розвідок у сфері інформаційних відносин доводить, що дослідники інформаційного права залишають за межами своїх розробок інститут охорони державної таємниці, обмежуючись лише висвітленням проблем порядку доступу до такої інформації [16 – 18].

Такий підхід до формування предмета інформаційного права зазнав критики з боку В. Ліпкана, який вважає неприпустимим формування інституту інформаційного права поза контекстом інформаційної безпеки. У контексті безпеки, на його переконання, стає онтологічним будь-яке питання, що розглядається в суспільстві. За таких умов інформаційне право, яке виступає регулятором даних суспільних відносин, у тому числі відносин у сфері безпеки, є взаємопов’язаним із усіма елементами інформаційного суспільства. А отже, інформаційна безпека, на думку цього науковця, є важливим і невід’ємним інститутом інформаційного права [19, с. 50-51].

Дійсно, аналіз вітчизняних і російських робіт з інформаційного права свідчить про неоднозначність розуміння не тільки предмета та об’єкта інформаційного права, а і його системи. Так, у російських наукових розвідках система інформаційного права структурно поділяється на дві частини – загальну і особливу, а в рамках останньої виокремлюються конкретні види таємниць. Щодо українських наукових праць, то подібна градація на частини відсутня, а вибір тем залежить від авторського усвідомлення змістовного наповнення інформаційного права. Але інформаційне право –

це досить молода наука, й тому немає нічого дивного, що її предмет та структура ще перебувають у стані невизначеності та постійного пошуку. Багатоваріантність підходів до цих проблем у науці може вважатися показником її розвитку та формування.

Інформаційна безпека може досліджуватися з позицій досить широкого спектра гуманітарних та технічних наук. Усі напрями таких досліджень мають “право на існування”, оскільки вирішують завдання, що ставляться сьогодні перед дослідниками. Не виключаємо, що окремі аспекти інформаційної безпеки належать до сфери інформаційного права. Проте намагання втиснути в предмет інформаційного права інститут інформаційної безпеки без пояснення конкретних завдань, які мають бути вирішені відповідно до предмету й методу цієї науки, є неприйнятним.

Інформаційна безпека є необхідною умовою існування особи, суспільства та держави. До сфери інформаційної безпеки держави входять конкретні дії щодо безпечних умов існуючих інформаційних процесів та забезпечення безпечних умов розвитку таких процесів у майбутньому. Це охоплює регулювання питань захисту самої інформації, захисту інформаційної інфраструктури держави, захисту інформаційного ринку та створення безпечних умов розвитку інформаційних процесів. Все це досягається проведенням необхідної державної політики інформаційної безпеки та створенням необхідних правових та організаційних засад [20, с. 101].

Слід зауважити, що в перших наукових дослідженнях проблем інформаційної безпеки питання охорони державної таємниці не розглядалися, оскільки інформаційна безпека зводилася до протидії комп’ютерній злочинності, інформаційному тероризму та спеціальним психологічним операціям. Зокрема, саме цим питанням була присвячена робота О. Литвиненка “Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії)”, де інформаційна безпека досліджувалася як складова національної безпеки України [21].

Поштовхом для розгляду питань щодо охорони державної таємниці в рамках інформаційної безпеки стала підготовка офіційного проекту Концепції національної безпеки України, розпочатої відповідно до Указу Президента України від 15 січня 1992 року № 41/92 та завершеної 10 березня 1992 року. Перше читання проекту Концепції у Верховній Раді України відбулося 19 жовтня 1993 року, друге – 24 травня 1996 року, а остаточне затвердження – 16 січня 1997 року [22]. У цьому документі вперше в законодавчій практиці України було встановлено визначення самих понять “національна безпека” та “національні інтереси”, а також окреслені основні сфери, завдання, напрямки та механізми їх захисту.

Згідно з концепцією, “національна безпека України як стан захищеності життєво важливих інтересів особи, суспільства і держави від внутрішніх і зовнішніх загроз є необхідною умовою збереження та примноження духовних і матеріальних цінностей” [22]. Ця принципова позиція стала основою формування подальшого бачення основних напрямків і загроз національній безпеці, у т.ч. і визначення інформаційної безпеки.

Найбільш поширеною думкою як в Україні, так і в більшості країн пострадянського простору стало визначення інформаційної безпеки як такого стану захищеності життєво важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму заподіяння шкоди через неповноту, несвоєчасність та недостовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації [23].

Дане тлумачення поняття інформаційної безпеки має своїм корінням законопроект “Про інформаційний суверенітет та інформаційну безпеку”, у статті 3 якого зазначено, що “інформаційна безпека України – це захищеність життєво важливих інтересів особи,

суспільства і держави, за якої виключається заподіяння їм шкоди через неповноту, невчасність і недостовірність інформації, через негативні наслідки функціонування інформаційних технологій або внаслідок поширення інформації, забороненої чи обмеженої для поширення законами України” [24]. Таким чином, у цьому законопроекті вперше була проголошена теза про те, що розголошення або несанкціонований витік забороненої чи обмеженої для поширення законами України інформації створює загрозу інформаційній безпеці держави.

Теоретичне підтвердження та розвиток окреслених у цьому законопроекті загроз інформаційній безпеці та чинників їх ескалації було зроблено експертами Українського центру економічних і політичних досліджень ім. О. Розумкова. Зокрема, ними був сформульований наступний перелік таких загроз:

– обмеження свободи слова та доступу громадян до інформації;

– руйнування системи цінностей, духовного та фізичного здоров’я особи, суспільства, негативні зміни їх цільових настанов;

– маніпулювання громадською думкою з боку державної влади, фінансово-політичних кіл;

– обмеження можливостей органів державної влади приймати адекватні рішення;

– порушення штатного режиму функціонування (руйнування) критично важливих інформаційних мереж, систем управління;

– несанкціонований витік таємної інформації, конфіденційної та іншої інформації з обмеженим доступом;

– спотворення, знищення інформаційних ресурсів, програмного забезпечення;

– низький рівень інтегрованості України у світовий інформаційний простір [25, с. 53].

Усі ці напрацювання стали підґрунтям для закріплення в статті 7 Закону України “Про основи національної безпеки України” від 19 червня 2003 року наступних загроз національним інтересам і національній безпеці України в інформаційній сфері:

– прояви обмеження свободи слова та доступу громадян до інформації;

– поширення засобами масової інформації культу насильства, жорстокості, порнографії;

– комп’ютерна злочинність та комп’ютерний тероризм;

– розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

– намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації [26].

З цього часу питання охорони державної таємниці та застосування обмежень щодо її обігу стали розглядатися у якості одного з напрямків інформаційної безпеки держави.

Так, у ґрунтовному дослідженні Б. Кормича “Інформаційна безпека: організаційно-правові основи” міститься окремий розділ “Організаційно-правові основи захисту та обмеження обігу інформації в цілях інформаційної безпеки”, один з підрозділів якого безпосередньо присвячений державній таємниці [20].

До охорони державної таємниці як одного із складових елементів забезпечення національної безпеки України підійшли також представники Національної академії СБ України у своїй колективній праці “Організаційно-правові основи захисту інформації з обмеженим доступом”. Зокрема, вони зазначили, що “суб’єкти, на яких покладено функції забезпечення національної безпеки, тією чи іншою мірою забезпечують і охорону державної таємниці” [27, с. 110].

Значний інтерес представляє також монографія О. Розвадовського “Забезпечення охорони державної таємниці та службової інформації: теоретичний, правовий та організаційний аспекти” [28], яка була покладена в основу його докторської дисертації, успішно захищеної за спеціальністю “Забезпечення національної безпеки”.

Огляд інших наукових розробок, які стосуються тих чи інших сфер охорони державної таємниці, дозволяє згрупувати їх за наступними напрямами досліджень даної проблематики:

1) організаційні засади секретного діловодства та порядок виготовлення, користування, збереження, передачі, транспортування та обліку матеріальних носіїв секретної інформації (С. Бервено, С. Князєв, О. Матяш, І. Севрюкова);

2) історія захисту інформації в Україні та провідних країнах світу (Б. Бернадський, О. Ботвінкін, В. Ворожко, А. Гуз, С. Князєв, О. Колєснік, А. Пашков, В. Сідак, В. Шлапачеко);

3) організація пропускного та внутрішньо-об’єктового режимів (С. Трофімов, М. Марченко);

4) порядок допуску та доступу до державної таємниці (А. Марущак, І. Романенко);

5) адміністративна відповідальність за порушення законодавства про державну таємницю (А. Благодарний, О. Нападистий, О. Розвадовський, С. Суслін);

6) кримінально-правова охорона державної таємниці (В. Шлапаченко, О. Шамсутдінов);

7) технічний захист інформації з обмеженим доступом (Л. Деркач, В. Паничек);

8) контррозвідувальний захист державної таємниці (М. Галамба);

9) захист інформації з обмеженим доступом країн-членів НАТО (В. Артемов, С. Князєв, А. Марущак, В.Панченко, В. Сідак, О. Шемякін).

Усі ці напрацювання відіграли суттєве значення в побудові діючої на даний час системи охорони державної таємниці та підготували наукове підґрунтя для подальшого дослідження цієї проблематики.

Висновки.

До розробки проблем охорони державної таємниці мають відношення багато галузей правової науки, але кожна з них розробляє свій, якийсь окремий аспект, певний елемент у системі охорони державної таємниці.

Зазначений підхід призводить до дублювання у дослідженнях одних і тих же питань різними правовими науками. При цьому теоретичні напрацювання у цій сфері розрізнені та несистематизовані, а окремі елементи системи охорони державної таємниці, які прямо не належать до предмета конкретної науки, розглядаються поверхнево, а тому незадовільно.

Кожен вид передумов (теоретичних, правових або емпіричних) має свої складові елементи і притаманне їм функціональне призначення.

Усі передумови взаємопов’язані й лише у своїй єдності уможливлюють побудову ефективної системи охорони державної таємниці.

Для створення надійної та ефективної системи охорони державної таємниці є цілком конкретні необхідні й достатні теоретичні, правові й емпіричні передумови, тому їх подальше накопичення призведе до затягування процесу створення такої системи.

Подальше дослідження проблем забезпечення охорони державної таємниці можливо лише в рамках комплексного дослідження, яке здатне виконати інтегративну функцію міждисциплінарних зв’язків тих галузей права, які вивчають різні аспекти діяльності з державної таємниці відповідно до своїх функціональних завдань.

Використана література

1. Великий тлумачний словник сучасної української мови ; уклад. і голов. ред. В.Т. Бусел. – К.-Ірпінь : ВТФ “Перун”, 2004. – 1440 с.

1. Зеленецкий В.С. Общая теория борьбы с преступностью. Концептуальные основы / В.С. Зеленецкий. – Х. : Основа, 1994. – 321 с.

2. Бунге М. Интуиция и наука / М. Бунге. – М. : Прогресс, 1967. – 187 с.

3. Карпович В.Н. Проблема, гипотеза, закон / В.Н. Карпович. – Новисибирск, 1980. – 176 с.

4. Бернал Дж. Наука в истории общества / Дж. Бернал. – М. : Издательство иностранной литературы, 1956. – 736 с.

5. Дурманов Н.Д. Государственная и военная тайна / Н.Д. Дурманов. – М. : Юриздат, 1942. – 16 с.

6. Беляев Н.А. Цели наказания и средства их достижения в исправительно-трудовых учреждениях / Н.А. Беляев . – Л. : Изд-во Ленинградского университета, 1963. – 186 с.

7. Стрельбицький М.П. Кадрова політика і робота з кадрами в умовах становлення української державності : монографія / М.П. Стрельбицький. – К. : ІПК СБУ, 1995. – 220 с.

8. Розанов И.С. Административно-правовые режимы по законодательству РФ, их назначение и структура // Государство и право. – 1996. – № 9. – С. 84-91.

9. Бахрах Д.Н. Административное право : учебник для вузов. – М. : Издательство ВЕК, 1999 – 368 с.

10. Тихомиров Ю.А. Административное право и процесс : полный курс / Ю.А. Тихомиров. – М. : Тихомирова М. Ю., 2001. – 652 с.

11. Ківалов С.В. Адміністративне право України : навч.-метод. посіб. / С.В. Ківалов, Л.Р. Біла. – [2-е вид., перероб. і доповн.]. – Одеса : Юрид. літ., 2002. – 312 с.

12. Административное право Украины : учеб. ; под ред. проф. Ю.П. Битяка. – [2-е изд., перераб. и доп.]. – Х. : Право, 2003. – 576 с.;

13. Крестьянинов А.А. Место таможенных режимов в системе административно-правовых режимов // Проблеми законності : респ. міжвідом. наук. зб. ; відп. ред. В.Я. Тацій. – Х., 1999. – Вип. 37. – С. 90-96.

14. Письменицкий А.А. Информационное право Украины / А.А. Письменицкий. – Х. : Бизнес Информ, 1996. – 208 с.

15. Марущак А.І. Правомірні засоби доступу громадян до інформації : навч. посіб. / А.І. Марущак. – Біло церква : Буква, 2006. – 432 с.

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

17. Марущак А.І. Інформаційне право України : підручник / А.І. Марущак. – К. : Дакор, 2011. – 456 с.

18. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / В.А.Ліпкан, В.Ю.Баскаков ; за заг. ред. В.А. Ліпкана. – К.: ФОП О.С. Ліпкан, 2013. – 344 с.

19. Кормич Б.А. Інформаційна безпека : організаційно-правові основи : навч. посібник. – К. : Кондор, 2008. – 384 с.

20. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): автореф. дис. на здобуття наук. ступеня політ. наук : спец. 23.00.04 “Політичні проблеми міжнародних систем та глобального розвитку” / О.В.Литвиненко. – К., 1997. – 18 с.

21. Про концепцію (основи державної політики) національної безпеки України : Постанова Верховної Ради України від 16.01.97 р. № 3/97-ВР // Відомості Верховної Ради України (ВВР). – 1997. – № 10. – Ст. 85.

22. Баранов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.

23. Про інформаційний суверенітет та інформаційну безпеку України : проект Закону України від 12.08.99 р. № 1207-d. – Режим доступу : http://www.rada.kiev.ua

24. Концепція (основи державної політики) інформаційної безпеки України : проект УЦЕПД // Національна безпека і оборона. – 2001. – № 1. – С. 2-59.

25. Про основи національної безпеки України : Закон України від 19.06.03 р.// Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст.351.

26. Організаційно-правові основи захисту інформації з обмеженим доступом : навч. посібник / [А.Б. Стоцький, О.І. Тимошенко, А.М. Гуз та ін.] ; за заг. ред. В.С. Сідака. – К. : Вид-во Європ. ун-ту, 2006. – 232 с.

27. Розвадовський О. Забезпечення охорони державної таємниці та службової інформації : теоретичний, правовий та організаційний аспекти : монографія : у 2-х ч. / О.Б. Розвадовський. – К. : Центр нав.-наук. та наук.-практ. видань НА СБ України, 2014. – (Ч. 1. – 228 с.; Ч. 2. – 284 с.).

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

Від редакційної колегії:

Указ Президента України №47/2017

Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року

“Про Доктрину інформаційної безпеки України”

Відповідно до статті 107 Конституції України, частини другої статті 2 Закону України “Про основи національної безпеки України” п о с т а н о в л я ю:

1. Увести в дію рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України” (додається).

2. Затвердити Доктрину інформаційної безпеки України (додається).

3. Цей Указ набирає чинності з дня його опублікування.

Президент України П. ПОРОШЕНКО
25 лютого 2017 року

ДОКТРИНА
інформаційної безпеки України

1. Загальні положення

Застосування Російською Федерацією технологій гібридної війни проти України перетворило інформаційну сферу на ключову арену протиборства. Саме проти України Російська Федерація використовує найновіші інформаційні технології впливу на свідомість громадян, спрямовані на розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України.

Комплексний характер актуальних загроз національній безпеці в інформаційній сфері потребує визначення інноваційних підходів до формування системи захисту та розвитку інформаційного простору в умовах глобалізації та вільного обігу інформації.

Принципи, пріоритети та напрями забезпечення кібербезпеки України визначені Стратегією кібербезпеки України, затвердженою Указом Президента України від 15 березня 2016 року № 96 “Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року “Про Стратегію кібербезпеки України”.

Доктрина інформаційної безпеки України (далі – Доктрина) визначає національні інтереси України в інформаційній сфері, загрози їх реалізації, напрями і пріоритети державної політики в інформаційній сфері.

Правовою основою Доктрини є Конституція України, закони України, Стратегія національної безпеки України, затверджена Указом Президента України від 26 травня 2015 року № 287 “Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року “Про Стратегію національної безпеки України”, а також міжнародні договори, згода на обов’язковість яких надана Верховною Радою України.

Терміни, що вживаються у Доктрині, мають таке значення:

стратегічні комунікації – скоординоване і належне використання комунікативних можливостей держави – публічної дипломатії, зв’язків із громадськістю, військових зв’язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави;

урядові комунікації – комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз’яснення урядової позиції та/або політики з певних проблемних питань;

кризові комунікації – комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації;

стратегічний наратив – спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію.

2. Мета та принципи Доктрини

Метою Доктрини є уточнення засад формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв’язаної нею гібридної війни.

Доктрина базується на принципах додержання прав і свобод людини і громадянина, поваги до гідності особи, захисту її законних інтересів, а також законних інтересів суспільства та держави, забезпечення суверенітету і територіальної цілісності України.

3. Національні інтереси України в інформаційній сфері

Національними інтересами України в інформаційній сфері є:

1) життєво важливі інтереси особи:

забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації;

забезпечення конституційних прав людини на захист приватного життя;

захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності у доступі до достовірної та об'єктивної інформації;

забезпечення вільного обігу інформації, крім випадків, передбачених законом;

розвиток та захист національної інформаційної інфраструктури;

збереження і примноження духовних, культурних і моральних цінностей Українського народу;

забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

зміцнення інформаційних зв’язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

розвиток системи стратегічних комунікацій України;

ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

формування позитивного іміджу України у світі, донесення оперативної, достовірної і об’єктивної інформації про події в Україні до міжнародної спільноти;

розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та у супутниковому мовленні за межами України.

4. Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері

Актуальними загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

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

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

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

інформаційне домінування держави-агресора на тимчасово окупованих територіях;

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

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

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

5. Пріоритети державної політики в інформаційній сфері

Пріоритетами державної політики в інформаційній сфері мають бути:

1) щодо забезпечення інформаційної безпеки:

створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них;

удосконалення повноважень державних регуляторних органів, які здійснюють діяльність щодо інформаційного простору держави, з метою досягнення адекватного рівня спроможності держави відповідати реальним та потенційним загрозам національним інтересам України в інформаційній сфері;

законодавче врегулювання механізму виявлення, фіксації, блокування та видалення з інформаційного простору держави, зокрема з українського сегмента мережі Інтернет, інформації, яка загрожує життю, здоров’ю громадян України, пропагує війну, національну та релігійну ворожнечу, зміну конституційного ладу насильницьким шляхом або порушення територіальної цілісності України, загрожує державному суверенітету, пропагує комуністичний та/або націонал-соціалістичний (нацистський) тоталітарні режими та їхню символіку;

визначення механізмів регулювання роботи підприємств телекомунікацій, поліграфічних підприємств, видавництв, телерадіоорганізацій, телерадіоцентрів та інших підприємств, установ, організацій, закладів культури та засобів масової інформації, а також використання місцевих радіостанцій, телевізійних центрів та друкарень для військових потреб і проведення роз’яснювальної роботи серед військ та населення; заборони роботи приймально-передавальних радіостанцій особистого та колективного користування і передачі інформації через комп’ютерні мережі в умовах запровадження правового режиму воєнного стану;

оптимізація законодавчих механізмів реалізації зобов’язань України в межах Європейської конвенції про транскордонне телебачення щодо держав, які не є підписантами зазначеної Конвенції;

створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку, насамперед у Збройних Силах України, з урахуванням практики держав – членів НАТО;

розвиток і захист технологічної інфраструктури забезпечення інформаційної безпеки України;

забезпечення повного покриття території України цифровим мовленням, насамперед у прикордонних районах, а також тимчасово окупованих територій;

розвиток цифрового мовлення, унеможливлення впливу на його інфраструктуру суб'єктів, що пов'язані з державою-агресором;

побудова дієвої та ефективної системи стратегічних комунікацій;

розвиток механізмів взаємодії держави та інститутів громадянського суспільства щодо протидії інформаційній агресії проти України;

боротьба з дезінформацією та деструктивною пропагандою з боку Російської Федерації;

посилення спроможностей сектору безпеки і оборони щодо протидії спеціальним інформаційним операціям, спрямованим на зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності, підрив обороноздатності України, деморалізацію особового складу Збройних Сил України та інших військових формувань, загострення суспільно-політичної ситуації;

виявлення та притягнення до відповідальності згідно із законодавством суб’єктів українського інформаційного простору, що створені та/або використовуються державою-агресором для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності;

унеможливлення вільного обігу інформаційної продукції (друкованої та електронної), насамперед походженням з території держави-агресора, що містить пропаганду війни, національної і релігійної ворожнечі, зміни конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України, провокує масові заворушення;

проведення розвідувальними органами України акцій сприяння реалізації та захисту національних інтересів України в інформаційній сфері, протидії зовнішнім загрозам інформаційній безпеці держави за межами України;

недопущення використання інформаційного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

2) щодо забезпечення захисту і розвитку інформаційного простору України, а також конституційного права громадян на інформацію:

стимулювання розвитку національного виробництва текстового і аудіовізуального контенту, зокрема шляхом створення системи квотування та проведення цільових конкурсів на надання грантів;

забезпечення функціонування Суспільного телебачення і радіомовлення України, у тому числі його належного фінансування;

створення системи мовлення територіальних громад, яка сприятиме розширенню комунікативних можливостей та зниженню конфліктності всередині громад;

підтримка вітчизняної книговидавничої справи, зокрема перекладів іноземних творів, забезпечення ними навчальних закладів і бібліотек;

розвиток правових інструментів захисту прав людини і громадянина на вільний доступ до інформації, її поширення, оброблення, зберігання та захист;

комплексна підтримка розвитку механізмів саморегуляції засобів масової інформації на засадах соціальної відповідальності;

підвищення медіа-грамотності суспільства, сприяння підготовці професійних кадрів для медіа-сфери з високим рівнем компетентності;

удосконалення законодавчого регулювання інформаційної сфери відповідно до актуальних загроз національній безпеці;

задоволення потреб населення тимчасово окупованих територій в об'єктивній, оперативній і достовірній інформації;

повне покриття території України цифровим та інтернет-мовленням замість аналогового і надання рівних можливостей доступу кожному громадянину до інформаційних ресурсів мережі Інтернет;

формування системи державної підтримки виробництва вітчизняного аудіовізуального продукту;

пропагування, у тому числі через аудіовізуальні засоби, зокрема соціальну рекламу, основних етапів і досвіду державотворення, цінностей свободи, демократії, патріотизму, національної єдності, захисту України від зовнішніх і внутрішніх загроз;

3) щодо відкритості та прозорості держави перед громадянами:

розвиток механізмів електронного урядування;

сприяння розвитку можливостей доступу та використання публічної інформації у формі відкритих даних;

інформування громадян України про діяльність органів державної влади, налагодження ефективної співпраці зазначених органів із засобами масової інформації та журналістами;

проведення реформи урядових комунікацій;

розвиток сервісів, спрямованих на більш масштабне та ефективне залучення громадськості до прийняття рішень органами державної влади та органами місцевого самоврядування;

сприяння формуванню культури суспільної дискусії;

4) щодо формування позитивного міжнародного іміджу України:

ґрунтовне реформування системи представлення інформації про Україну на міжнародній арені;

розвиток публічної дипломатії, у тому числі культурної та цифрової;

активізація скоординованої інформаційної роботи закордонних дипломатичних установ України;

сприяння поширенню та розвитку системи іномовлення України;

створення та забезпечення функціонування правового механізму взаємодії державних органів з інститутами громадянського суспільства з метою інформаційної підтримки комерційної, гуманітарної, просвітницької, культурної та іншої діяльності таких інститутів за межами України;

постійний моніторинг пропаганди держави-агресора, розроблення та оперативна реалізація адекватних заходів протидії;

недопущення використання міжнародного інформаційного простору в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні;

реформування системи взаємовідносин з українською діаспорою шляхом забезпечення більш тісної співпраці та проведення ефективних заходів, зокрема в рамках комунікацій “від людини до людини”;

участь у міжнародних культурних заходах з метою представлення національної культури та ідентичності;

запровадження міжнародних культурних фестивалів в Україні з метою популяризації української культури та розвитку комунікацій «від людини до людини».

6. Механізм реалізації Доктрини

Рада національної безпеки і оборони України відповідно до Конституції України та у встановленому законом порядку має здійснювати координацію діяльності органів виконавчої влади щодо забезпечення національної безпеки в інформаційній сфері.

Кабінет Міністрів України забезпечуватиме здійснення інформаційної політики держави, фінансування програм, пов'язаних з інформаційною безпекою, спрямовуватиме і координуватиме роботу міністерств, інших органів виконавчої влади у цій сфері.

На Міністерство інформаційної політики України мають бути покладені в установленому порядку організація та забезпечення:

моніторингу засобів масової інформації та загальнодоступних ресурсів вітчизняного сегмента мережі Інтернет з метою виявлення інформації, поширення якої заборонено в Україні;

моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері;

сприяння Міністерству закордонних справ України щодо донесення офіційної позиції України до іноземних засобів масової інформації;

формування поточних пріоритетів державної інформаційної політики, контролю їх реалізації;

координації діяльності центральних та місцевих органів виконавчої влади у сфері забезпечення інформаційного суверенітету України;

урядових комунікацій;

кризових комунікацій, зокрема під час проведення антитерористичної операції та в особливий період;

вжиття заходів в інформаційній сфері, пов’язаних із запровадженням правових режимів надзвичайного чи воєнного стану;

розроблення стратегічного наративу і його імплементації;

вироблення і впровадження стратегії інформаційного забезпечення процесу звільнення та реінтеграції тимчасово окупованих територій;

розроблення та впровадження єдиних стандартів підготовки фахівців у сфері урядових комунікацій для потреб державних органів.

Для сприяння координації діяльності органів виконавчої влади у сфері забезпечення інформаційного суверенітету України та взаємодії з іншими державними органами в інформаційній сфері у Міністерстві інформаційної політики України може утворюватися в установленому порядку допоміжний орган.

На Міністерство закордонних справ України має бути покладено в установленому порядку:

формування та реалізацію стратегії публічної та культурної дипломатії України;

координацію інформаційної діяльності державних органів у зовнішньополітичній сфері;

забезпечення просування інтересів України за кордоном інформаційними засобами;

забезпечення донесення позиції України до керівництва іноземних держав, парламентів та урядів, зовнішньополітичних відомств, представників бізнесу та експертних кіл, широкої громадськості, сприяння просуванню позитивного іміджу України;

сприяння просуванню українських телеканалів у кабельні та супутникові мережі за кордоном;

забезпечення налагодження взаємодії з міжнародними партнерами як на двосторонній, так і на багатосторонній основі з метою застосування міжнародного досвіду та найкращих практик у контексті протидії інформаційним загрозам.

Міністерство оборони України має забезпечувати функціонування системи військово-цивільних зв’язків у місцях постійної дислокації та розгортання підрозділів Збройних Сил України, інших військових формувань, а також організовувати і забезпечувати:

Зв’язки з українськими та іноземними засобами масової інформації щодо висвітлення ситуації в районі проведення антитерористичної операції в Донецькій та Луганській областях;

протидію спеціальним інформаційним операціям, спрямованим проти Збройних Сил України та інших військових формувань;

супроводження інформаційними засобами виконання завдань оборони України;

донесення достовірної інформації до військовослужбовців Збройних Сил України, інших військових формувань, зокрема через засоби масової інформації Збройних Сил України.

Міністерство культури України, Державне агентство України з питань кіно, Національна рада України з питань телебачення і радіомовлення, Державний комітет телебачення і радіомовлення України відповідно до компетенції братимуть участь у забезпеченні захисту українського інформаційного простору від пропагандистської

аудіовізуальної та друкованої продукції держави-агресора; розроблятимуть пріоритети і стимули розвитку українського кіно, телевізійного контенту, книгодрукування, зокрема висвітлення героїчного спротиву Українського народу російській агресії.

Служба безпеки України у межах компетенції має здійснювати:

моніторинг спеціальними методами і способами вітчизняних та іноземних засобів масової інформації та мережі Інтернет з метою виявлення загроз національній безпеці України в інформаційній сфері;

протидію проведенню проти України спеціальних інформаційних операцій, спрямованих на підрив конституційного ладу, порушення суверенітету і територіальної цілісності України, загострення суспільно-політичної та соціально-економічної ситуацій.

Розвідувальні органи України у процесі здійснення розвідувальної діяльності мають сприяти реалізації та захисту національних інтересів України в інформаційній сфері за кордоном, протидіяти зовнішнім загрозам інформаційній безпеці держави.

Державна служба спеціального зв’язку та захисту інформації України забезпечуватиме в межах компетенції формування і реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом України.

Національний інститут стратегічних досліджень має забезпечити науково-аналітичне та експертне супроводження процесу формування і реалізації державної інформаційної політики.

7. Прикінцеві положення

Зважаючи на особливі умови і ведення проти України агресивної інформаційної війни не лише на її території, але й у світі, забезпечення реалізації Доктрини можливе лише за умови належної координації заходів, здійснюваних усіма державними органами. Ключові заходи відповідно до положень Доктрини визначатиме Рада національної безпеки і оборони України.

Суб'єкти реалізації державної інформаційної політики у взаємодії з інститутами громадянського суспільства в межах компетенції забезпечують реалізацію Доктрини, а також за необхідності вносять обгрунтовані пропозиції щодо корегування її положень.

Глава Адміністрації Президента України І. РАЙНІН

До відома авторів

“**ІНФОРМАЦІЯ І ПРАВО**” – 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 інформаційного права, правової інформатики, інформаційної і національної безпеки та інформації в інших галузях права в умовах становлення інформаційного суспільства.

Зміст матеріалів статей має бути спрямований на вирішення визначених автором наукових завдань згідно з такими напрямами досліджень:

- **Інформаційне право.**
- **Правова інформатика.**
- **Інформаційна і національна безпека.**
- **Інформація в інших галузях права.**

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 – до 15 стор. (або за рішенням редколегії).*

   Стаття має передбачати такі обов’язкові структурні елементи:
   - *УДК.*
   - *Ім’я та прізвище, науковий ступінь, вчене звання автора, місце роботи.*
   - *Назва статті.*
   - *Анотація та ключові слова – укр., рос., англ. мовами.*
   - ***Розв’язання проблеми:***
     - **постановка проблеми** *(загальна характеристика) та аналіз досліджень (публікацій), в яких започатковано розв’язання проблеми, виділення не вирішених її частин, котрим присвячується стаття;*
     - **формування мети** *(постановка завдання) статті;*
     - **виклад основного матеріалу** *– вирішення завдання та обґрунтування результатів.*
   - **Висновки, пропозиції** *за результатами розв’язання проблеми.*
   - *Перспективи щодо 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 280 грн. на рахунок Інституту**.

Реквізити для оплати робіт: *Науково-дослідний інститут інформатики і права Національної академії правових наук України. Р/р 31251259111870 в Державній казначейській службі України МФО: 820172, ЄДРПОУ: 25959933 (з приміткою – за науковий журнал).*
Адреса редакції: 01032, м. Київ, вул. Саксаганського, 110-В.

Копію квитанції прохання направити на е-адресу: bvm777@ukr.net

Д о у в а г и

- Редакційна колегія не завжди поділяє погляди авторів публікацій. Статті видаються в авторській редакції.
- Редакційна колегія залишає за собою право на:
  – відхилення матеріалів статей, які не відповідають тематиці журналу, або таких, які виконані з порушенням зазначених вимог до оформлення статей та Відгуків;
  – внесення до статті змін редакційного змісту у зв’язку зі скороченням обсягу матеріалу.

*** * * * * * * * * ***

ІНФОРМАЦІЯ І ПРАВО

НАУКОВИЙ ФАХОВИЙ ЖУРНАЛ

№ 1(20)

2017

Засновники журналу:	- Науково-дослідний інститут інформатики і права Національної академії правових наук України; - Національна бібліотека України ім. В.І. Вернадського Національної академії наук України; - Відкритий міжнародний університет розвитку людини “Україна”.
Видавець:	© Науково-дослідний інститут інформатики і права Національної академії правових наук України.
Адреса редакції:	01032, м. Київ, вул. Саксаганського, 110-В. НДІ інформатики і права НАПрН України. Тел.: 234-94-56; e-mail: bvm777@ ukr.net
Веб-сторінки журналу у мережі Інтернет:	//www.ippi.org.ua – (НДІ інформатики і права НАПрН України); //www.nbuv.gov.ua – (Нац. бібліотека України ім. В.І. Вернадського).