

Національна академія правових наук України
Науково-дослідний інститут інформатики і права
Секція права національної безпеки та військового права

Національний технічний університету України
«Київський політехнічний інститут імені Ігоря Сікорського»
Навчально-науковий центр інформаційного права
та правових питань інформаційних технологій

Навчально-науковий центр прав і безпеки людини
в інформаційному суспільстві
Науково-дослідного інституту інформатики і права НАПрН України та
Національного педагогічного Університету імені М. П. Драгоманова

Наукова лабораторія інформаційно-правових проблем
інноваційного розвитку та освіти
Науково-дослідного інституту інформатики і права НАПрН України та
Вінницького Державного педагогічного університету імені Михайла Коцюбинського

ЗАХИСТ ПРАВ, СВОБОД І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В СУЧАСНИХ УМОВАХ

МАТЕРІАЛИ
ДРУГОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

21 травня 2020 року

Київ-2020

Захист прав, свобод і безпеки людини в інформаційній сфері
3 38 **в сучасних умовах:** Матеріали другої науково-практичної конференції.
21 травня 2020 р., м. Київ. / Упоряд. : С.О. Дорогих, В.Ф. Фурашев,
В.Г. Пилипчук, О.В. Петришин. – Київ, 2020. – 376 с.
ISBN 978-617-7814-68-8

Матеріали конференції присвячені розгляду теоретико-правових та практичних питань захисту прав, свобод і безпеки людини в інформаційній сфері у сучасних умовах.

Для спеціалістів у сферах правотворення, правозастосування та правоохоронної, вчених, фахівців та експертів різних галузей права, науково-педагогічних працівників, аспірантів, докторантів, студентів вищих навчальних закладів, а також усіх, хто цікавиться реальними та потенційними суспільно-правовими тенденціями і проблемами наслідків сучасного науково-технічного прогресу в інформаційній сфері, своєчасного та належного правового супроводження цих процесів, а також забезпечення прав, свободи і безпеки людини під час поводження з інформацією на сучасному етапі розвитку національного та світового суспільства.

У конференції взяли участь провідні експерти і вчені наукових установ і навчальних закладів, представники зацікавлених державних органів та громадських організацій.

Матеріали подано у авторській редакції.

Рекомендовано до друку:

*Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України.*

Протокол № 5 від 21.05.2020 р.

ISBN 978-617-7814-68-8

© Науково-дослідний інститут інформатики
і права НАПрН України, 2020

© Національний технічний університет України
«Київський політехнічний інститут
імені Ігоря Сікорського», 2020

© Національний педагогічний Університет
імені М. П. Драгоманова, 2020

© Вінницький Державний педагогічний
університет імені Михайла Коцюбинського,
2020

© Колектив авторів

ЗМІСТ

Пилипчук В.Г.

ПРОБЛЕМИ ЗАХИСТУ ПРИВАТНОСТІ,
ПРАВ І БЕЗПЕКИ ЛЮДИНИ
В СУЧАСНИХ УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ..... 11

Довгань О.Д.

ЩОДО ДЕЯКИХ АСПЕКТІВ ПРАВ, СВОБОД ТА БЕЗПЕКИ
ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ 18

Андрусишин Б.І., Опольська Н.М.

ОБМЕЖЕННЯ ПРАВА НА СВОБОДУ ТВОРЧОСТІ
НА ЕТАПІ УТВЕРДЖЕННЯ ТОТАЛІТАРНОГО РЕЖИМУ
В УКРАЇНІ (1917 – 1939 РР.) 28

Корж І.Ф.

ПРАВА І БЕЗПЕКА ЛЮДИНИ В СУЧАСНИХ УМОВАХ 37

Золотар О.О.

БЕЗПЕКА І ПРАВА ДИТИНИ В ЧАСИ ПАНДЕМІЇ
(НА ПРИКЛАДІ ФРАНЦІЇ)..... 44

Гордієнко С.Г.

СТАН І ПЕРСПЕКТИВИ
ВИВЧЕННЯ ТА АНАЛІЗУ ПРАВОВИХ
АСПЕКТІВ ЖИТТЄВОГО ЦИКЛУ ІНФОРМАЦІЇ..... 49

Солодка О.М.

СВОБОДА ІНФОРМАЦІЇ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ
ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ..... 54

Бєлєвцева В.В.

ПРАВОВІ ЗАСАДИ МЕХАНІЗМУ ЗАХИСТУ
ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД ЛЮДИНИ
В УКРАЇНІ..... 59

Солончук І.В.

ІНФОРМАЦІЙНЕ СУДОЧИНСТВО: РЕАЛІЗАЦІЯ ПРАВА НА СУДОВИЙ ЗАХИСТ ПРАВ, СВОБОД ТА ІНТЕРЕСІВ ОСОБИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ	65
--	----

Ткачук Н.І.

ОКРЕМІ ПИТАННЯ ЩОДО НАЦІОНАЛЬНИХ ТА МІЖНАРОДНИХ ЗАСАД ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД ЛЮДИНИ	73
---	----

Забара І.М.

АКТУАЛЬНІ ПИТАННЯ БЕЗПЕКИ І ЗАХИСТУ ПРАВ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИННИХ ЗАХОДІВ: ОЦІНКИ, ПОЗИЦІЯ Й ІНІЦІАТИВИ ООН	77
---	----

Юник І. Г.

РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ ТА ВІДКРИТОСТІ ВЛАДНИХ ІНСТИТУЦІЙ	82
---	----

Ірха Ю.Б.

ПРАВОВА ПОІНФОРМОВАНІСТЬ НАСЕЛЕННЯ УКРАЇНИ ЯК ОДНА З ГАРАНТІЙ ДОСТУПУ ГРОМАДЯН ДО ПРАВОСУДДЯ	87
--	----

Богущкий П.П.

ІНФОРМАЦІЙНА ПРИВАТНІСТЬ І ПУБЛІЧНІСТЬ ЯК СУТНІСНІ ОЗНАКИ ІНФОРМАЦІЙНО-ПРАВОВИХ КОМУНІКАЦІЙ	95
---	----

Баранов О.А.

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА КІБЕРБЕЗПЕКА	101
---	-----

Дзьобань О.П.

АДАПТАЦІЯ ЛЮДИНИ ДО УМОВ СУЧАСНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА: БЕЗПЕКОВІ ПРОБЛЕМИ	110
--	-----

Беланюк М.В.

ПРАВА ЛЮДИНИ В ІНТЕРНЕТ	116
-------------------------------	-----

Арістова І.В.

ОХОРОНА ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ В УКРАЇНІ	123
--	-----

Тарасюк А.В.

МОРАЛЬНО-ЕТИЧНІ ЗАСАДИ У КІБЕРБЕЗПЕЦІ ЛЮДИНИ	130
---	-----

Білоус О.А.

ЗАПОБІГАННЯ КОРУПЦІЇ У ПРЕДСТАВНИЦЬКИХ ОРГАНАХ ВЛАДИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ	135
---	-----

Єсімов С. С.

СУЇЦИДАЛЬНА ПОВЕДІНКА ТА ІНТЕРНЕТ	141
---	-----

Конотопенко О.П., Лапшин С.А.

ПУБЛІЧНА ІНФОРМАЦІЯ І ВІДКРИТІ ДАНІ ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ ПРАВ І БЕЗПЕКИ ГРОМАДЯН В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ.....	147
--	-----

Гіляка О.С.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ОКРЕМИХ ПРАВ ЛЮДИНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....	154
--	-----

Кононенко В.В.

ЗАХИСТ ПРАВ ТА СВОБОД ГРОМАДЯН В УМОВАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ	160
--	-----

Маньгора В.В.

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ
КІБЕРБУЛІНГУ В СУЧАСНИХ УМОВАХ..... 166

Проць І.М.

ТЕНДЕНЦІЇ РОЗВИТКУ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО
БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ В УКРАЇНІ 172

Доронін І.М.

ІНТЕРЕСИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ,
ЯК ПІДСТАВА ДЛЯ ОБМЕЖЕННЯ
ПРАВ І СВОБОД ЛЮДИНИ,
У СУЧАСНОМУ ПОЛІТИКО-ПРАВОВОМУ КОНТЕКСТІ..... 177

Ткачук Т.Ю.

СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ..... 183

Калиновський Ю.Ю.

ЦІННІСНА БЕЗПЕКА ЛЮДИНИ
В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ..... 190

Батиргарєєва В.С.

ІНФОРМАЦІЙНИЙ ПРОСТІР
ЯК ПРОВОКУЮЧИЙ ЧИННИК
У ДЕТЕРМІНАЦІЇ ВЧИНЕННЯ ЗЛОЧИНІВ 197

Радзієвська О.Г.

НАЦІОНАЛЬНИЙ НАРАТИВ В УМОВАХ ПРОВЕДЕННЯ
ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ..... 202

Гаврильців М.Т.

ВИКЛИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ
В УМОВАХ ГІБРИДНОЇ ВІЙНИ ТА НАПРЯМИ
УДОСКОНАЛЕННЯ ЗАСАД ФУНКЦІОНУВАННЯ
СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 208

Косогов О.М.

СТРАТЕГІЇ ТА СПОСОБИ НЕГАТИВНИХ ІНФОРМАЦІЙНИХ
ВПЛИВІВ ЯК СКЛАДОВИХ НЕПРЯМИХ ДІЙ
В УМОВАХ МІЖДЕРЖАВНИХ КОНФЛІКТІВ 215

Ковалів М.В.

РОЛЬ ТЕХНІЧНИХ ГАРАНТІЙ ПРАВ ЛЮДИНИ
ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 222

Лепіш Н.Я.

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНЕ ПРОТИБОРСТВО
ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ 226

Кронівець Т.М.

ЗАХИСТ ПРИВАТНОСТІ ЖИТТЯ ЛЮДИНИ
В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ:
ОСОБЛИВОСТІ ПОНЯТІЙНОГО АПАРАТУ 230

Яременко О. І.

ПРАВОВІ ЗАСАДИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ
ФІЗИЧНИХ ОСІБ ЯК СУБ'ЄКТІВ ВІРТУАЛЬНИХ
ІНФОРМАЦІЙНИХ ВІДНОСИН..... 234

Проць І.М., Чабак В.Ю.

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
У КОНТЕКСТІ СУЧАСНОЇ КОМУНІКАЦІЇ..... 241

Брайчевський С.М.

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ
В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ
В УМОВАХ РЕЖИМНИХ ЗАХОДІВ..... 245

Дранник В.А.

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ
ДАНИХ ГРОМАДЯН 251

Уханова Н.С.

ЗАРУБІЖНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ПРАВОВОГО
РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ
У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ..... 253

Вальчук О.І., Петрик В.В.

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ
ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ АПАРАТУ
ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ
З НАДЗВИЧАЙНИХ СИТУАЦІЙ..... 259

Julia V. Strebkova

REVIEW OF BIOPOLITICS NORMS IN ADJUSTMENT
OF REPRODUCTION IN UKRAINE 263

Грищук А.Б.

ІНФОРМАЦІЙНО-ПРАВОВІ СКЛАДОВІ ІНТЕГРУВАННЯ
КУРСІВ ЕЛЕКТРОННОГО НАВЧАННЯ
У НАВЧАЛЬНИЙ ПРОЦЕС ПРОФЕСІЙНОЇ ПІДГОТОВКИ
ДЕРЖАВНИХ СЛУЖБОВЦІВ В УКРАЇНІ..... 267

Мельник Е.А., Конотопенко О.П., Пилипенко Т.І.

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА КОМПЕТЕНТНІСТЬ
КЕРІВНИКА В УМОВАХ ТРАНСФОРМАЦІЇ
СИСТЕМИ ВИЩОЇ ОСВІТИ..... 275

ЗАХИСТ ПРАВ, СВОБОД І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИНУ

Фурашев В.М.

ІНФОРМАЦІЙНЕ ПРАВО ТА ПАНДЕМІЯ
КОРОНОВІРУСУ COVID-19: ЗВ'ЯЗОК ТА НАСЛІДКИ 282

Денисенко Н.В.

ОБМЕЖЕННЯ ПРАВ ЛЮДИНИ ПІД ЧАС КАРАНТИНУ:
ЧИ ІСНУЄ ЗАГРОЗА ДЕМОКРАТІЇ?..... 285

Щириця Т.

МОРАЛЬНО-ЕТИЧНІ АСПЕКТИ ЗАХИСТУ ПРАВ ЛЮДИНИ
В ІНФОРМАЦІЙНІЙ СФЕРІ ЗА УМОВ КАРАНТИНУ 292

Проць І.М., Ямкова Т.І.

ЗАХИСТ ІНФОРМАЦІЙНИХ ПРАВ
ПІД ЧАС КАРАНТИНУ 295

Лапишин С.А., Гриб В.І.

ОСОБЛИВОСТІ ПОДАННЯ ДОКУМЕНТІВ
ДЛЯ ЗДОБУТТЯ СТУПЕНЮ ВИЩОЇ ОСВІТИ МАГІСТРА
В УМОВАХ КАРАНТИНУ
(НА ПРИКЛАДІ РЕЄСТРАЦІЇ НА ЄВІ)..... 301

Лапишин С.А., Конотопенко О.П.

ОСОБЛИВОСТІ ПРОВЕДЕННЯ КОНКУРСУ
НА ЗАМІЩЕННЯ ВАКАНТНИХ ПОСАД В ОРГАНАХ
ВИКОНАВЧОЇ ВЛАДИ УКРАЇНИ
У ПЕРІОД КАРАНТИНУ 306

СТОРІНКА МОЛОДОГО ВЧЕНОГО

Безкоровайна Н.М.

ПЕРЕДУМОВИ ЗАСТОСУВАННЯ
ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА
У СФЕРІ КІБЕРБЕЗПЕКИ НА МІСЦЕВОМУ РІВНІ 313

Власова І.А.

ХАРАКТЕРИСТИКА ЗАРУБІЖНОГО ДОСВІДУ
РЕФОРМУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ:
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИЙ АСПЕКТ..... 320

Добжанська М.Є.

ІНФОРМАЦІЙНА СКЛАДОВА УПРАВЛІННЯ
СФЕРОЮ КУЛЬТУРИ: МІЖНАРОДНІ ВІДНОСИНИ..... 325

Іванова А.В.

КАДРОВА БЕЗПЕКА

В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ..... 332

Кравчук К., Засць Т.

УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПРОЦЕСАМИ

В КАРАНТИННО-ОБМЕЖУВАЛЬНИХ УМОВАХ

В СИСТЕМІ СЕРЕДНЬОЇ ТА ВИЩОЇ ШКОЛИ:

ПОРІВНЯЛЬНИЙ АНАЛІЗ..... 338

Мар'яш В.Ю.

ПОСАДИ В СИСТЕМІ

ДЕРЖАВНОГО УПРАВЛІННЯ УКРАЇНИ.

ПРОБЛЕМНІ ПИТАННЯ КЛАСИФІКАЦІЇ ПОСАД» 346

Тишківська А.В.

ВИКОРИСТАННЯ ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ ЄДЕБО

В КОНТЕКСТІ БЕЗПЕКИ ЛЮДИНИ

В ІНФОРМАЦІЙНІЙ СФЕРІ (НА ПРИКЛАДІ ВДПУ) 350

Франко Л.І., Франко І.О.

ПУБЛІЧНЕ АДМІНІСТРУВАННЯ ЗАКЛАДІВ

ОХОРОНИ ЗДОРОВ'Я В УМОВАХ КАРАНТИНУ 355

Чинник П.А.

ПРАВО НА ІНФОРМАЦІЙНУ ПРИВАТНІСТЬ 358

Черненко Д.С.

ЦИФРОВА ГРАМОТНІСТЬ

ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ 365

Якубовська Я.В.

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ

В ІНФОРМАЦІЙНІЙ СФЕРІ

В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ ВЛАДИ В УКРАЇНІ..... 369

Пилипчук В.Г.

доктор юридичних наук, професор,
член-кореспондент НАПрН України,
директор Науково-дослідного інституту інформатики і права НАПрН України

ПРОБЛЕМИ ЗАХИСТУ ПРИВАТНОСТІ, ПРАВ І БЕЗПЕКИ ЛЮДИНИ В СУЧАСНИХ УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Особисті права і свободи людини, як відомо, є невід'ємними від безпеки людини, суспільства і держави. За цих умов актуально постає проблема пошуку балансу між захистом приватності, у тому числі інформаційної приватності життя людини, та потребами захисту інформаційної і національної безпеки. Тобто, в умовах правової держави та розвитку інформаційного суспільства мають бути законодавчо визначені обмеження довільного поводження з правами людини, зокрема в інформаційній сфері.

Вказана проблема значно актуалізувалася в сучасних умовах цифрових трансформацій та введення надзвичайної ситуації, пов'язаної з карантинно-обмежувальними заходами, що сприяло виявленню низки важливих питань, які потребують термінового опрацювання.

Результати аналізу захисту прав, свобод і безпеки людини в інформаційній сфері дають змогу виокремити низку **системних проблем**, зокрема:

1) проблема **захисту приватного життя** людини.

Розвиток цієї ідеї знайшов відображення у так званій концепції «права на приватність» (right to privacy) – права особи «на саму себе», права «бути залишеною на самоті» (privacy). За матеріалами узагальнення прецедентної практики в США «делікти проти приватності» (privacy torts) було розділено на такі групи:

- *втручання в усамітненість (intrusion upon seclusion)* – вторгнення в «особистий простір» індивіда;
- *публічне розголошення інтимних фактів (publication of private facts)*;

- спотворене представлення особи перед громадськістю (*false light*);
- використання чужого імені або образу в корисливих цілях (*appropriation*).

Зазначене, як видається, також дає підстави для окремого розгляду питання щодо запровадження у науковий обіг поняття **«інформаційна приватність»**;

2) проблема **негативних інформаційно-психологічних впливів** на людину і суспільство.

Вказана проблема набула актуальності протягом останніх років в умовах гібридної війни та інформаційної агресії проти України. Характерним є й те, що методи інформаційної війни нині активно застосовуються проти низки країн-членів ЄС і НАТО.

За цих обставин український досвід набуває підвищеної уваги, оскільки підтверджує, що цільове застосування інформаційних та психологічних операцій може призвести до виникнення психологічної залежності людини від новітніх цифрових технологій та інформаційно-комунікаційних мереж, поширення негативного інформаційного впливу на великі групи осіб, провокування суспільних конфліктів і втрати територіальної цілісності.

З урахуванням зазначеного, як видається, потребує окремого комплексного опрацювання **проблема масового інформаційно-психологічного впливу на людину і групи осіб, суспільство та міжнародну спільноту**, що виникав у умовах запровадження у більшості країн світу надзвичайної ситуації або надзвичайного стану, пов'язаних з пандемією COVID-19;

3) проблема захисту **безпеки приватних персональних даних** та імплементації відповідних стандартів ЄС в національне законодавство згідно з «Пакетом захисту даних ЄС». Цим пакетом визначено такі основні **принципи обробки персональних даних: законність, справедливість і прозорість; цільове обмеження; зведення до мінімуму даних; точність; обмеження зберігання; цілісність і конфіденційність**.

Варто зауважити, що в Україні ефективна система захисту персональних даних практично відсутня (*це сталося після внесення змін до законодавства у 2011 – 2013 рр.*). При цьому, функції парламентського контролю та центрального органу виконавчої влади було по-

кладено на Уповноваженого Верховної Ради України з прав людини, що не відповідає вимогам Конституції України і законодавства ЄС.

Останні події, пов'язані з масовим витоком персональних даних громадян України через інформаційно-комунікаційні мережі підтверджують актуальність цієї проблеми і нагальну необхідність внесення змін до законів України «Про інформацію», «Про захист персональних даних» та Кримінального кодексу України. Зазначене також дає підстави для окремого розгляду питання щодо запровадження у науковий обіг визначення поняття «**безпека приватних персональних даних**».

Розглянемо питання щодо розуміння понять «інформаційна приватність» та «безпека приватних персональних даних».

Як відомо, життя, бажання, мрії та діяльність людини завжди були пов'язані зі словосполученням «недоторканність особистого життя», еквівалентом якого у законодавстві США та публічних виданнях країн-членів ЄС є поняття «*privacy*» (від англ. «**приватність**»). Цей термін є запозиченням значення з латинської мови слів: особистість, інтимність, таємність, самотність, власність, міжособисті відносини [1].

Узгодженого та юридичного визначення поняття «*privacy*» немає. Зустрічаються його різні розуміння і тлумачення, зокрема: «особисте життя», «право на приватне життя», «недоторканність приватного життя», «право на самоту» [2]. В українській «Юридичній енциклопедії» термін «*privacy*» визначено як «*приватна справа, таємниця, усамітненість*» – правова категорія в англосаксонській правовій системі, пов'язана із захистом інтимного життя людини [3].

Як вважається, історія *приватності* та безпосередньо пов'язаної з нею *конфіденційності інформації* має понад 3000 років, а в сучасному розумінні – лише близько 150 років. Вона свідчить, що приватність раніше завжди була другорядною, оскільки на практиці потреба у виживанні завжди затьмарювала бажання усамітнення[4]. Нині приватність розглядається як фундаментальне право людини й перебуває в одному ряді із правом на життя, свободою переконань, власністю на майно та особисті здобутки на результаті інформаційної та інтелектуальної праці.

Фахівці громадських організацій Electronic Privacy Information Center та Privacy International у своєму спільному дослідженні запропонували умовно виокремити такі **види приватності** [5]:

- *фізична приватність* – умови захисту від примусових для людини процедур, зокрема медичних та ін. Деякі міри обумовлені потребами врахування інтересів суспільства і держави. Зокрема, поліції надане право зняти в арештованого відбитки пальців або узяти в нього аналіз ДНК для включення в національну базу даних тощо;

- *територіальна і майнова приватність* – зазвичай мається на увазі недоторканність фізичних речей та житла. Певний рівень приватності мають не тільки будинки і квартири, але й робочі місця, готельні номери, купе поїзда тощо. Майнова приватність визначається правом власності на майно та правом використання об'єктів інтелектуальної власності. Право власності на інформаційний продукт законодавством не визначається, хоча інформацією завжди торгували і вона знаходиться у комерційному у обігу;

- *інформаційна приватність* – під цим розуміється наявність передусім захисту прав людини та основоположних свобод в інформаційній сфері, її уявлень та намагань покращити своє життя;

- *приватність комунікацій* – це все, що пов'язане з технічними засобами і техніко-технологічними діями, які стосуються, зокрема, таємниці телефонних розмов, поштових, електронних повідомлень. Приватність комунікацій безпосередньо пов'язана з інформаційною приватністю, зокрема з Інтернетом, який, як ніколи раніше, надає можливості несанкціонованих контролю та впливу на особисте життя людини.

Інформаційна приватність завжди займала особливе місце у стосунках між людьми. Її основою є забезпечення захисту відомостей про людину, насамперед, у контексті нецільового і несанкціонованого отримання та використання її персональних даних.

Виокремлюють такі **основні складові права на інформаційну приватність**: право на самотність; право на інтимність; право на анонімність; право контролювати інформацію про себе [6], право «бути забутим» [7].

Також слід зауважити, що в українському законодавстві відсутнє юридичне визначення понять «приватність» та «приватні персо-

нальні дані». Однак, вони згадуються у ст. 182 Кримінального кодексу України та у нормативному акті Кабінету Міністрів України «Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль» від 31 серпня 2016 р. № 0108. Зокрема, ст. 8 «Захист персональних даних» Угоди визначає: *«Сторони зобов'язуються вживати необхідних заходів відповідно до національного законодавства у сфері охорони **приватних персональних даних** з метою захисту персональних даних українських громадян, відібраних для тимчасового працевлаштування відповідно до цієї Угоди, у тому числі від випадкової їх втрати, пошкодження, незаконної обробки та доступу»*[8].

Як свідчать результати аналізу, нині також відсутні єдині підходи щодо розуміння понять «*приватні персональні дані*» та «*безпека приватних персональних даних*». В сучасних умовах поширення інформаційно-комунікаційних систем і мереж забезпечення інформаційної приватності дедалі більше ускладнюється. Загальновідомим є те, що будь-які відомості або дані про людину можуть бути отримані завдяки Інтернет-ресурсам та використані не лише на її користь, а також у протиправних цілях (для маніпулювання свідомістю, шантажу, залякування, агресивної реклами, інформаційного насилля тощо). Зазначене безпосередньо стосується проблеми захисту інформаційної приватності та безпеки приватних персональних даних, які є невід'ємною складовою забезпечення інформаційної і національної безпеки.

Відповідно до Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» термін «*інформаційна безпека*» означає *стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації*.

Згідно з Доктриною інформаційної безпеки України [9] до ключових ознак інформаційної безпеки віднесено:

1) *конфіденційність* – стан поводження з інформацією, при якому доступ до неї отримують тільки суб'єкти, які мають на це право;

2) *цілісність* – запобігання несанкціонованій або незаконній модифікації інформації;

3) *доступність* – запобігання тимчасовому або постійному приховуванню інформації від користувачів, які мають право на доступ.

Враховуючи зазначене **безпеку приватних персональних даних** можемо розглядати як стан захищеності конфіденційних відомостей (даних) про особу та процес забезпечення їх захисту.

Загалом, підсумуємо розглянуте такими основними висновками:

1. В умовах розбудови глобального інформаційно-комунікаційного простору, розвитку телекомунікаційних систем і мереж та сучасних цифрових трансформацій актуалізується проблема пошуку єдиних підходів і законодавчого визначення або уточнення у міжнародних і національних нормативно-правових актах необхідного категоріально-понятійного апарату, зокрема, термінів «*приватність*», «*інформаційна приватність*», «*приватні персональні дані*», «*безпека приватних персональних даних*» тощо. Водночас, потребує уточнення і юридичного закріплення перелік конфіденційних відомостей про особу, на які мають поширюватися правові гарантії захисту, а також розроблені й запроваджені ефективні цифрові системи технічного захисту вказаних відомостей.

2. Актуальною міжнародною проблемою, зокрема, для країн-членів ЄС і держав, які є асоційованими членами або співпрацюють з ЄС, є подальший пошук балансу між захистом прав і свобод людини, зокрема, з питань інформаційної приватності й безпеки приватних персональних даних, та потребою суспільства, держави й міжнародної спільноти у безпеці. Баланс між захистом приватності та потребою у безпеці є досить складним питанням, яке в епоху інформатизації та цифрових трансформацій не може вирішуватися на підставі поглядів минулого часу.

3. Мірою оцінки суджень про допустимість втручання в особисте (приватне) життя людини може бути: а) *право приватної власності людини на свої персональні дані*; б) *контроль використання особою інформації про себе*; в) *визначені законом випадки обмеження приватності життя людини, пов'язані із захистом національ-*

ної безпеки, боротьбою зі злочинністю, захистом прав і свобод інших осіб; г) базові принципи «Пакету захисту даних ЄС» (2016 р.).

Література

1. Прохвачева О. (2000) Лингвокультурный концепт “приватность”. URL:<http://www.dissercat.com/content/lingvokulturnyi-kontsept-privatnost-na-materiale-amerikanskogo-varianta-angliiskogo-yazyka#ixzz3AMsvTYM>
2. Большой англо-русский словарь; под ред. проф. И.Р. Гальперина. Москва, 1988 г.
3. Юридична енциклопедія: в 6 т.; редкол. Ю.С. Шемшученко (голова редкол.) та ін.. Київ: «Українська енциклопедія», 2003. Т.5: П-С. С. 53.
4. Приватность: рождение и смерть. 3000 лет истории приватности. URL: <https://www.habr.com/ru/company/parallels/blog/348922>
5. Privacy & Human Rights. Privacy International and Electronic Privacy Information Center, 1999. URL: [//www.epic.org](http://www.epic.org); Смирнов С. Приватность. Москва: Изд. “Права человека”. 2002. 95 с. С. 9.
6. Соколова М. (2014). Защита персональных данных онлайн: основные понятия. URL: https://www.researchgate.net/publication/281459597_Zasita_personalnyh_dannyh_onlajn_osnovnye_ponatia
7. Становлення і розвиток правових основ та системи захисту персональних даних в Україні: монографія; за ред. В.М. Брижка, В.Г. Пилипчука. Київ: ТОВ “Видавничий дім “АртЕк”, 2017. 226 с. С. 85-98; Брижко В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. Київ: НДІП НАПрН України, 2019. 290 с. С. 164-175.
8. “Про ратифікацію Угоди між Кабінетом Міністрів України та Урядом Держави Ізраїль про тимчасове працевлаштування українських працівників в окремих галузях на ринку праці Держави Ізраїль” від 31.08.16 р. № 0108. URL: http://www.w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=59911
9. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року “Про Доктрину інформаційної безпеки України”: Указ Президента України від 25.02.17 р. № 47/2017. URL: <https://www.president.gov.ua/documents/472017-21374>

Довгань О.Д.

доктор юридичних наук, професор,
заслужений діяч науки і техніки
України,
перший заступник директора
з наукової роботи НДІП НАПрН
України

ЩОДО ДЕЯКИХ АСПЕКТІВ ПРАВ, СВОБОД ТА БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ

Загальновизнані права людини і громадянина в сфері інформації у демократичному суспільстві виступають основним критерієм, що характеризує стан інформаційної безпеки конкретної особи і суспільства в цілому. Насамперед це пов'язано з одним із основних пріоритетів інформаційної політики будь-якої країни - дотриманням балансу відповідних інтересів особистості, суспільства і держави. Країни, що обрали демократичний шлях розвитку, принципово виходять при цьому з примату прав і свобод особистості.

На нормативному рівні це зазвичай виражається у конституційних гарантіях свободи слова та доступності інформації для кожного громадянина (свобода публічних висловлювань незалежно від їхнього політичного змісту; забезпечення безперешкодного отримання громадянами повної та неупередженої інформації). Обмеження цього фундаментального права особистості розглядається як виняток із загального принципу відкритості інформації та реалізується тільки відповідно до чинного законодавства і лише в окремих випадках.

Основний закон виступає гарантом зазначених положень. Зокрема, його стаття 3 проголошує: «Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю. 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].

Що стосується права, для нього важливі насамперед ті риси (властивості, ознаки) людини, які ним охороняються. Насамперед, це найвищі соціальні цінності: життя, здоров'я, свобода, честь, гідність, безпека. У цьому випадку людина виступає, перш за все як суб'єкт прав і свобод та об'єкт їх забезпечення.

Ключовими для визначення прав і свобод людини в галузі інформації є норми статей 34 і 32 Конституції України.

Так, ст. 34 Конституції визначає право на свободу слова та право на інформацію, згідно з яким:

- кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань;
- кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір.

Здійснення цих прав може бути обмежене законом (ч. 3 ст. 34 Конституції) в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

Гарантії права людини на невтручання в особисте життя, ґрунтуються насамперед на ст. 32 Конституції, яка, зокрема, визначає, що: *«Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини»*.

Нормами цієї статті визначаються і основні механізми забезпечення зазначеного права. Першим із них (ч. 3 ст. 32 Конституції) є право громадянина ознайомлюватися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Це право дає змогу встановити сам факт збирання інформації про особу органами публічної влади та їх посадовими

особами, визначити їх зміст і на підставі цього установити ступінь правомірності таких дій. Інший механізм (ч. 4 ст. 32 Конституції) полягає в *гарантії судового захисту прав*:

- спростовувати недостовірну інформацію про себе і членів своєї сім'ї;
- вимагати вилучення будь-якої інформації;
- відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Похідним від права на невтручання в особисте життя є *право на таємницю кореспонденції*, оскільки фактично цим правом встановлюється додаткова гарантія невтручання в особисте життя людини.

В рамках Конвенції про захист прав і основоположних свобод людини [2] (ст. 8) ці права розглядаються в комплексі.

В Конституції України це право визначено окремою ст. 31, за якою кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Основним механізмом забезпечення цього права є визначене в ст. 8 правило, згідно з яким винятки із права на таємницю кореспонденції можуть бути встановлені лише судом з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо.

Новим значущим явищем, що вплинуло на зміни в інформаційній сфері, стала 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 [3].

Без сумніву, Великі дані та штучний інтелект – ключ до важливих інновацій. Вони мають неймовірний потенціал визначати економічні показники та суспільний прогрес. У демократіях неприпустимо, щоби з допомогою цих технологій пригноблювали людей. Проте різні установи зловживають їхніми особистими даними, контролюючи їхню поведінку, а це – ознака тоталітаризму. Така по-

ведінка не лише несумісна з правами людини та демократичними принципами, а й непридатна для сучасного, інноваційного управління суспільством. Наука намагається знайти відповідь на запитання, як використовувати «інформацію для людства», тобто великі дані та штучний інтелект – на благо суспільства [4].

Постає питання яким чином можна протистояти втручанню в особисте життя цифрових технологій? Насамперед, зауважимо, що передусім, в часи цифрової революції, як і раніше, діє базове право громадян на захист, що є основою сучасної, демократичної спільноти.

Так, право на приватність (*право на недоторканність приватного та сімейного життя*) передбачено в Конституції України та конкретизовано у відповідних статтях українського законодавства.

Зокрема, частина 1 статті 32 Конституції містить загальне положення про захист особистого і сімейного життя і заборону державі втручатися в нього, крім випадків передбачених Конституцією. У свою чергу, стаття 30 Основного закону гарантує недоторканність житла, тоді як його стаття 31 безпосередньо регулює таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Частина 2 статті 31 Конституції України забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, частина 3 статті 28 Конституції України забороняє піддавати особу без її вільної згоди медичним, науковим чи іншим досліддам.

Інші аспекти та елементи права на приватність розкриваються в Цивільному Кодексі України, Кримінальному кодексі України, спеціальних законах та нормах, наприклад «Про захист персональних даних».

Зауважимо, що в умовах стрімкого науково-технічного прогресу, особливо в інформаційній сфері, надзвичайно актуальним постає питання забезпечення персональних даних, оскільки воно торкається кожного з нас.

Згаданий вище Закону України «Про захист персональних даних», саме спрямований на регулювання правових відносин, пов'язаних із захистом і обробкою персональних даних, із забезпеченням захисту основоположних прав і свобод людини і громадя-

нина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних.

До речі, Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру [5] (підписана в Страсбурзі 28 січня 1981 р.) у своїй ст. 1 закликає до забезпечення на території кожної держави-учасниці для кожної особи незалежно від її національності або помешкання поважання її прав і основних свобод, зокрема її права на недоторканність особистого життя, стосовно автоматизованої обробки даних особистого характеру.

Крім того, у резолюції Генеральної Асамблеї ООН «Право на приватність у цифрову епоху» [6] від 18 грудня 2013 року підкреслено глобальну й відкриту природу Інтернету і швидкий розвиток у сфері інформаційних та комунікаційних технологій як рушійної сили для прискорення прогресу на шляху до розвитку в різних формах. У документі підтверджено, що «ті ж права, що люди мають в оффлайн-режимі, повинні також бути захищені онлайн, у тому числі право на приватність».

Засади захисту персональних даних у правовій практиці країн ЄС зводяться до такого: пріоритетним є право особи розпоряджатися своїми персональними даними, а їх використання без дозволу володільця тягне відповідальність згідно з законодавством; для будь-кого, хто здійснює користування персональними даними фізичних осіб з їх дозволу, встановлено відповідальність у разі умисного розголошення цих даних третім особам (*крім випадків, коли на це надано дозвіл*).

Нові правила захисту персональних даних (GDPR) [7], які набули чинності у 2018 році є обов'язковими для країн-членів ЄС. Крім того, вони поширюються і на компанії з інших країн, які пропонують товари і послуги в ЄС.

У нових правилах переглянуті цивільні права користувачів, відповідальність за збереження даних, а також введені деякі обмеження переміщення даних між різними країнами. Важливим нововведенням є запровадження більш суворого покарання за несвоєчасне повідомлення інформації про виток даних.

Обов'язковим є необхідність отримання згоди користувачів на обробку їх персональних даних, причому на обробку даних з різни-

ми цілями потрібні будуть окремі згоди. При цьому, згода має бути вільною, свідомою і конкретною, а також може бути відкликана в будь-який момент. Не буде вважатися вільною згода, якщо користувач змушений її дати, щоб одержати доступ до сайту, програми або додатка. Виняток - персональні дані користувача потрібні для виконання угоди. У випадках, коли персональні дані збираються й обробляються для маркетингових цілей, користувач повинен мати можливість не погоджуватися зі збором і обробкою його даних.

Компанії, що працюють із персональними даними, повинні будуть також вести облік операцій з персональними даними (*тип даних і цілі, для яких вони обробляються*), мінімізувати використання персональних даних відповідно до принципу *data protection by design*, а також проводити внутрішній аудит.

Заслуговує на увагу також одна із особливостей метафізики права – людиноцентризм [8]. Право має відійти від забезпечення інтересів тих, хто його створює і цілковито бути відданим служінню людині. Безперечно тільки людина, її природні права мають бути центром гуманізації та оптимізації правової системи. Принцип «*Salus populi suprema lex est*¹» має стати чітким орієнтиром сучасної правової системи.

Серед системи природніх прав, особливе місце займає право на інформацію. Спірність включення даного права до природніх є сумнівною. Адже виходячи із загальноприйнятих особливостей природнього права людини (надані людині від природи; носять природний і невідчужуваний характер; виступають у якості найвищої соціальної цінності; є безпосередньо діючим правом; знаходяться під захистом держави; відповідають міжнародним стандартам) право на інформацію цілком відповідає згаданим критерієм.

Розвиваючи дану думку, слід окремо підкреслити, що на основі права на інформацію відбувається осмислення права людиною як елемента формування безпечного середовища проживання. Це пояснюється тим, що при здійсненні будь-якої фізичної або інтелектуальної діяльності людина завжди стикається з інформацією: процесом її отримання, обробки, структурування, та навіть прийняття будь-якого рішення потребує інформаційної підтримки.

¹ благо народу - вищий закон

Таким чином будь-яка діяльність людини є процесом пізнання. У цьому процесі пізнання людина, багато в чому, через інстинкт самозбереження намагається всі явища або об'єкти, які їй невідомі зрозуміти і пояснити в своїй свідомості на основі отриманої інформації. Фактично, людина з'ясовує їх ступінь небезпеки для себе та суспільства в цілому. Цим, людина формує безпечне середовище для своєї життєдіяльності, що в загальному, можна назвати відображенням її біологічної природи. Таким чином «народжується» категорія «інформаційна безпека людини, суспільства, держави». Окреслені процеси і є відображенням метафізичного у праві.

Отже, можна з упевненістю стверджувати, що з правом на інформацію тісно пов'язана інша системоутворююча категорія – «інформаційна безпека». Більше того, право на інформацію виступає певним індикатором її стану. Адже це найочевидніший елемент у порівнянні з іншими (інформаційна безпека суспільства, інформаційна безпека держави). Більше того, при порушенні права на інформацію людини, тобто зазіхання на інформаційну безпеку людини, інформаційна безпека суспільства і держави однозначно будуть піддаватися негативному впливу як від загроз із зовні так і внутрішніх загроз.

Отже, оскільки головним джерелом добробуту людини стає інформація, то інформаційна безпека людини повинна забезпечити збереження цілісності особи та її здатності до розвитку як визначальних категорій буття людини, враховуючи реалії становлення інформаційного суспільства. Але нажаль, існує низка питань, і ми погоджуємося з автором [9], які потребують врегулювання на законодавчому рівні, і пов'язані саме з інформаційною безпекою людини:

- створення правової основи для освіти протягом життя, як необхідної умови існування людини в інформаційному суспільстві;
- врегулювання питань щодо надання психологічної і психотерапевтичної допомоги, а також інших видів послуг, що використовують методи інформаційно-психологічного впливу;
- підвищення поінформованості громадян про свої права і свободи через формальні джерела інформації;
- ефективне регулювання ЗМІ, особливо нових медіа з метою забезпечення дотримання стандартів журналістської діяльності;

– створення умов для розвитку критичного мислення та оволодіння іншими інструментами, життєво необхідними в умовах інформаційного суспільства, особливо у вразливих категорій населення – дітей та молоді, осіб похилого віку, осіб з особливими потребами; цю потребу особливо актуалізує інформаційна війна;

– подолання цифрової нерівності в географічному та демографічному (віковому) вимірі та інші.

Що стосується питань безпеки людини, то в Конституції України (ст. 3) безпека людини визначається однією з найважливіших соціальних цінностей. Безпека є найнеобхіднішою із потреб людини. Це насамперед пов'язано з тим, що людина постійно дбає про збереження своїх прав і свобод від тих чи інших посягань, небезпечних явищ, прагне до безпеки, бо це благо є вічною природною потребою, умовою для життєдіяльності людини.

Безпека людини – це об'єктивний стан і суб'єктивне відчуття фізичної, майнової, соціальної (матеріальної), психологічної і моральної захищеності людини, її прав і свобод. Людина лиш тоді перебуває у безпеці, коли вона, її права і свободи надійно захищені (забезпечені, гарантовані). Інакше кажучи, *саме права і свободи людини та їх гарантії і забезпечують її безпеку* [10].

Надійна безпека для всіх людей може бути досягнута лише через усунення причин створення загроз для людини, її прав і свобод. Тільки в умовах демократичної, соціальної, правової держави людина знаходить безпеку від тиранії, гноблення, свавілля, беззаконня, безправ'я, насильства тощо.

Головною функцією, метою і обов'язком нашої держави, усіх гілок влади та державного механізму є забезпечення безпеки людини (*гарантування, охорона і захист прав і свобод людини*). Держава є основним суб'єктом забезпечення безпеки людини. Саме людина, її права і свободи є головним об'єктом національної, державної, політичної, техногенної, екологічної, економічної, інформаційної, громадської безпеки (*захисту від злочинів та криміналітету*).

Таким чином, вбачається, що потреба в безпеці – це потреба в захищеності й потреба почувати себе у стані, за якого відсутня загроза для життя і здоров'я. Безпека – це умова задоволення інших потреб. Людина прагне до безпеки, намагається жити в без-

пеці, в стані, коли їй ніщо не загрожує, у світі, вільному від страху. Але в суспільстві існують небезпеки для людини: фізичні, біологічні, психологічні, екологічні, економічні, соціологічні, інформаційні, політичні тощо. Деякі з них, на жаль, стають нормою нашого життя.

Норми щодо дотримання інформаційних прав і свобод людини містяться, насамперед, в Конституції України, міжнародно-правових актах з прав людини, галузевих міжнародних та національних правових актах, якими врегульовані окремі питання інформаційних прав людини. Ці норми потрібно дотримуватися і виконувати.

Тому, у подальшому, виходячи з положень статей 3 та 21 Конституції України, які визначають природне право початком і основою української правової системи, необхідно дотримуватися двох напрямків: правоохоронного, який полягає у можливості реалізації прав і свобод людини, та правозахисного щодо захисту порушених суб'єктивних прав. Метою останнього повинно бути упередження, припинення правопорушення та відновлення бажаних для людини, суспільства або держави прав і свобод, встановлених нормативно-правовими актами.

Захист приватності та його рівень має бути таким, щоб як можна більше мінімізувати загрози особистої безпеки в інформаційному суспільстві. Оскільки, традиційних правових засобів та інструментів у сучасному світі недостатньо для того, щоб вирішити проблеми приватності, тому потрібно зосередитися на правових механізмах запобігання вторгнень до приватного життя, розробці гнучкої правової бази, критеріїв можливого втручання до приватності та його межах в інформаційному суспільстві.

Крім того, гарантування безпеки особи, суспільства і держави від зовнішніх та внутрішніх загроз в інформаційній сфері, потребує формування сучасних ефективних механізмів забезпечення інформаційної безпеки, які відповідатимуть характеру і масштабам викликів сьогодення, а також створення належних умов реалізації державної політики, спрямованої на захист національних цінностей та реалізацію національних інтересів України.

Література

1. Конституція України від 28 червня 1996 року // Відом. Верховної Ради України. – 1996. – № 30. – Ст. 141.
2. https://www.echr.com.ua/wp-content/uploads/2018/02/Convention_UKR.pdf
3. Довгань О.Д. Право на приватність у цифрову епоху/ О.Д. Довгань // Інформаційно-правове та організаційно-управлінське забезпечення інноваційного розвитку регіону: Матеріали круглого столу / 7 червня 2019 р., м. Вінниця / ВДПУ, НДІП НА-ПрН України, К., Видавничий дім «АртЕк» – 2019.
4. <https://zbruc.eu/node/44988>
5. https://zakon.rada.gov.ua/laws/show/994_326
6. General Assembly Resolution “The right to privacy in the digital age”, A/RES/68/167
7. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних : Збірник документів ; [неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука]. - (Науково-дослідний інститут інформатики і права Національної академії правових наук України). - К. : ТОВ “Видавничий дім “АртЕк”, 2018.- 180 с.
8. Довгань О.Д. Наукова рефлексія інформаційної безпеки України: від позитивізму до метафізики права / О.Д. Довгань, Т.Ю.Ткачук // Інформація і право № 4 (27). – 2018 . – С. 79-89.
9. Інформаційна безпека людини: теорія і практика: Монографія. / Золотар О. О. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.
10. Довгань О.Д. Права і безпеки людини: правові норми / Довгань О.Д. // Права, свободи і безпека людини в інформаційній сфері: Матеріали науково-практичної конференції. 10 травня 2018 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. – Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2018. – 174 с.– С. 17-20.

Андрусишин Б.І.

доктор історичних наук, професор,
декан факультету політології
та права Національного
педагогічного університету імені
М.П. Драгоманова

Опольська Н.М.

кандидат юридичних наук, доцент,
завідувач кафедри права
Вінницького національного
аграрного університету

ОБМЕЖЕННЯ ПРАВА НА СВОБОДУ ТВОРЧОСТІ НА ЕТАПІ УТВЕРДЖЕННЯ ТОТАЛІТАРНОГО РЕЖИМУ В УКРАЇНІ (1917 – 1939 РР.)

Початковий етап комуністичного будівництва має важливе значення в історії правового регулювання свободи творчості. Українські творці опинилися у складному становищі через те, що переважна їх більшість сповідували загальнодемократичні принципи, прагнули свободи слова, свободи творчості, вони були вільними у своїх переконаннях і висловлюваннях. В той період в Україні були створені геніальні художні твори, літератури та мистецтва, гідні світового визнання. Відбувся переворот в естетичній свідомості. Українська творчість за змістом і формами, під гаслами свободи, духовного оновлення, національного відродження стала наближеною до європейського рівня. Цьому сприяло те, що культурна розбудова більшовицького режиму спочатку підтримала розпочату УНР і Гетьманатом П. Скоропадського українізацію і начебто об'єдналася з культурною революцією.

Упродовж першого десятиліття більшовицького режиму в Україні культурне будівництво визнавалось третім фронтом соціалістичної роботи, поряд з фронтами військовим та господарським. Третім він був і за порядком, і за вагою, і за значенням. Протягом 1920-х рр. було досягнуто певних позитивних результатів. Діяли десятки науково-природничих, технічних і суспільствознавчих

товариств. Митці об'єднувалися в творчі об'єднання, яких було більше 40, зокрема: «Плут» (спілка селянських письменників), «Молодняк» (спілка молодих письменників), «АСПИС» (Асоціація письменників), «Ланка», «МАРС» (Майстерня революційного слова), «ВАПЛІТЕ» (Вільна академія пролетарської літератури), «Авангард», «Нова генерація» та ін. На 1929 р. існувало 61 товариство і організація [1, с.128].

Першим централізованим органом цензури в Україні було Всеукраїнське державне видавництво, яке з лютого 1920 року підпорядковувалось Всеукраїнському центральному виконавчому комітету УСРР. Орган отримував право надавати дозвіл на друкування всієї періодичної преси, видань різних установ і організацій. У травні 1921 року воно було перейменоване на Державне видавництво України (ДВУ) і передано у підпорядкування Наркомату освіти. Йому додатково надали контроль за розповсюдженням друкованої продукції [2, с.46-47]

Виконуючи вказівки московського керівництва колегія агітпропвідділу ЦК КП(б)У 29 квітня 1922 року вирішила створити при Головному політико-освітньому комітеті Головне управління у справах друку з губернськими відділеннями по місцях. Створений 6 червня 1922 р. РНК РСФСР Головліт розглядав територію УСРР як свою юрисдикцію [3, с.32-37]. У Києві, Одесі, Харкові передбачалося відкрити місцеві відділення Головліту РСФСР. Українське керівництво сприйняло це як пряме втручання у справи суверенної республіки.

На самій зорі становлення більшовицького режиму позиція партійного керівництва позначилася певною толерантністю. В постановках Політбюро КЦ КП(б)У 1924-1927 рр. йшлося: «ні одна з існуючих, зокрема літературних організацій...не може претендувати на монопольне проведення партійної лінії в цій ділянці...партія в цілому ні в якому разі не може зв'язати себе прихильністю до якого небудь напряму в галузі літературної форми; так само недопустимою є затвердження декретом або партійною постановою легалізована монополія на літературно-видавничу справу. Партія повинна всемірно викорчовувати спроби свавільного і некомпетентного адміністративного втручання в літературні справи», що є достатньо показовим [1, с.129].

29 серпня 1922 року Радою народних комісарів УСРР створив український цензурний орган – Центрального управління у справах друку (ЦУСД), що входив до структури Народного комісаріату освіти. Проведена в 1930 році реорганізація всіх республіканських Головлітів надавала їм право на відкриття видавництв і здійснення контролю над ними. Постанова ВЦВК і РНК УСРР «Про затвердження устави про Головне управління в справах літератури та видавництв і його місцеві органи» від 1931 року основним завданням діяльності Головліту визначало: «Здійснювати всі види політично-ідеологічного, воєнного і економічного контролю над призначеними до оголошення або поширення творами друку, рукописами, книжками, плакатами, картинами тощо, а так само над радіомовленням, лекціями, виставками» [3, с.32-37].

Відбувалось утвердження тоталітарного режиму, внаслідок чого, українські митці сповна відчували на собі дії радянської репресивної машини, були фізично знищені, або морально зламані. Відкритий доступ до біографічних довідок багатьох українських митців, які були тривалий час засекречені, закінчуються словом «розстріляний». Багато митців, науковців стали жертвами сталінського терору. Є. Гедройць цей період назвав «Розстріляним відродженням» [4]. Практично вперше в період незалежної України в рамках забезпечення освітнього процесу поняття «Розстріляне відродження» ввів Б. Андрусишин [5, с.39].

Вільні українські творці опинилися в маховику більшовицької пропаганди та репресій. Інтелігенцію, творчих особистостей, які займали активну громадянську позицію, що суперечила «диктатурі пролетаріату» було фізично знищено, розстріляно без суду і слідства, визнано «ворогами народу», репресовано.

В цей період спостерігається великий розрив між реальним становищем творців та нормативно-правовою базою, яка регулювала свободу творчості. Декларативно-вербальному проголошенню свободи совісті, свободи вираження власних поглядів, свободи зібрань у Конституції Української Соціалістичної Радянської Республіки, прийнятої 14 березня 1919 р. Всеукраїнським Центральним Виконавчим Комітетом [6] суперечило впровадження плану монументальної пропаганди. Було створено систему партійно-державного

керівництва культурним життям. Агітаційно-пропагандистський відділ ЦК РКП(б) ліквідував свободу друку, націоналізував видавничу справу, кіноіндустрію, театри, музеї, організував агітбригади та агітттеатри, знімали агітфільми. Для пропаганди революційних ідей та нової ідеології ефективно використовували політичні плакати, у створенні яких брали участь відомі художники, поети [7].

Визначальною у сфері творчої діяльності стала комуністична пропаганда, лише така творчість вважалась істинною. Право на творчу діяльність отримували лише ті особи, які служили культу Леніна, що у 1930-х рр. доповнився культом Сталіна.

На зламі 1920–30-х рр. національна складова України зазнала вже не просто утисків, а й нещадних руйнувань, що означало її фактичний кінець. Кремлівський централізм з його донедавна інтернаціоналістичною риторикою і фразеологією остаточно перейшов до російсько-шовіністичної стратегії, що означало перетворення культурної революції на знаряддя сталінського тоталітаризму [8].

Нищівні зміни інтелектуально-ідеологічної сфери отримали назву «культурна революція». Головною метою культурної революції, яка, на відміну від індустріалізації і колективізації, не повинна була закінчуватися ніколи, проголошувалося створення нової людини. І нова культура, і маси «нових людей» були необхідні для зміцнення більшовицького режиму [7].

25 листопада 1922 р. було введено в дію Кодекс Законів про народну освіту УРСР, який проголосив право всіх громадян УРСР на вільний доступ до науки, рівно як до знань та мистецтва, у всіх культурно-освітніх закладах держави [9].

Майже одночасно з суто вербальним проголошенням свободи творчості було організовано один із перших таборів ГУЛАГу – 13 жовтня 1923 р. у на Соловецьких островах у Білому морі. За офіційними даними, у перші десять років існування «Соловецького лагерь особого назначения» (СЛОНу) тут загинуло 7,5 тисячі осіб. Насправді, як стверджують історики, жертв було набагато більше. Лише в одному Соловецькому етапі, страчено у Сандармосі чекистом із сільською двокласною освітою капітаном НКВС Матвеевим, було 1111 в'язнів. У списку – відомі світу культурні і державні діячі та науковці: режисер і творець українського модерного театру

Лесь Курбас, прозаїки і поети Микола Вороний, Микола Зеров, Мислав Ірчан, Григорій Епик, Павло Филипович, перекладач і філософ Валер'ян Підмогильний, попередник Нобелівських лауреатів Камю і Сартра – драматург Микола Куліш, чий п'єси йшли у Москві, Варшаві, Парижі й Нью-Йорку, президент харківської Вільної академії пролетарської літератури Михайло Яловий, професори Степан Рудницький і Сергій Грушевський, академік Матвій Яворський, міністр УНР Антін Крушельницький разом з двома синами, міністр фінансів УСРР Михайло Полоз та інші [10].

Звинувачення в українському націоналізмі стало підґрунтям політичних переслідувань творців та науковців радянської України. Більшовицький режим, борючись із «дрібнобуржуазною національною ідеологією», вдавався до політичних переслідувань, репресій.

Друга Конституція УРСР, яка була прийнята 15 травня 1929 р. проголошувала свободу висловлювання поглядів трудящих через усунення залежності друку від капіталу, а також передбачала передачу в руки робочого класу та селян усіх технічних і матеріальних засобів видання газет, книг, інших форм друку, забезпечення по всій країні їх вільного поширення[11].

Норми Конституції УРСР мали декларативний характер і не були нормами прямої дії. Це було декларативно-вербальне визнання свободи творчої діяльності на конституційному рівні, законодавча симуляція, яка в реальному житті не мала механізму реалізації. Саме в цей період спостерігається найбільший розрив між проголошеною свободою слова, вираження своїх поглядів та реальним забезпеченням свободи творчості. Придушення ідейно-політичної опозиції, опору інтелігенції, науковців, творців унеможливлювали реалізацію права на свободу творчості.

Сучасні документально-публіцистичні, наукові праці розкривають реальні умови життя творців. Внаслідок голоду 1932-1933 рр. загинуло приблизно 10 мільйонів осіб. В творчості літераторів та художників, які пережили жахливі 1932-1933 роки можна побачити багато творів, віршів, картин, які нагадують про геноцид українського народу - Голодомор[8].Боротьба радянської влади проти ворогів народу в першу чергу була спрямована на українську інтелігенцію, творців, художників, митців.

Ситуація, яка складалася на той час у суспільно-політичному та економічному житті країни, зокрема набирання обертів маховиком репресій, аж ніяк не сприяла літературній творчості. На зміну літературному плюралізмові з його розмаїттям течій і напрямків, літературних організацій та їхніх друкованих органів йшов «казьонний» оптимізм «соціалістичного реалізму» [13, с.16-17].

«Чистка» 1933– 1934 рр. охопила також і науково-дослідні установи республіки. «Органи державно-політичного управління викрили і звільнили Всеукраїнську Асоціацію марксистсько-ленінських науково-дослідних інститутів (1931– 1936) від цілої групи контрреволюціонерів» – зазначалося в одній з тогочасних публікацій. Безліч інтелігентів – вихідців з України «недержавної», що віддавали свої знання та працю для відродження державної України та майбутнього возз'єднання всіх українських земель, загинули внаслідок сталінських репресій [13, с.16-17].

Період Великого терору – найменування доби, коли сталінські репресії були ще більше посилені і фактично зведені до максимуму, супроводжується прийняттям Конституції УРСР 1937 р., стаття 124 якої декларативно проголошувала «У відповідності з інтересами трудящих і з метою зміцнення соціалістичного ладу громадянам УРСР гарантується законом: а) свобода слова, б) свобода друку, в) свобода зборів і мітингів, г) свобода вуличних походів і демонстрацій. Ці права громадян забезпечуються наданням трудящим і їх організаціям друкарень, запасів паперу, громадських будинків, вулиць, засобів зв'язку і інших матеріальних умов, необхідних для їх здійснення» [14].

5 серпня 1937 року за наказом НКВС СРСР № 00447 набула чинності Постанова ЦК ВКП(б) «Про антирадянські елементи», яку теоретично обґрунтував новий нарком НКВС Єжов та відредагував сам Сталін. З цього дня розпочалася наймасовіша «чистка» радянського суспільства від елементів, що «не годилися для будівництва комунізму». У кожному республіку, область і район спускалися ліміти на репресування за I і II категоріями (I – розстріл, II – ув'язнення, співвідношення один до трьох). Радянський політв'язень, письменник Василь Овсієнко зазначає, що ці ліміти не просто виконувалися, а й з радістю перевиконувалися, каральні органи запрошу-

вали їх збільшення. З таким проханням у Москву тричі звертався нарком внутрішніх справ УСРР Ізраїль Леплевський, а після його розстрілу – двічі в.о. наркома Олександр Успенський. Найбільша провина вільнолюбних та хазяйновитих українців була в тому, що сталінському режиму не вдавалося перетворити їх на «зразкових» радянських громадян. За архівними даними, в Україні з 1935-го по 1951 рік жертвами розкуркулення стали понад 2 мільйони 800 тисяч осіб [10].

Кількість жертв репресій, депортацій і голоду в Україні за часи радянської влади не піддається підрахунку. Це приблизно третина українського народу. Американський дослідник української трагедії Джеймс Мейс писав, що нинішня Україна – це соціологічно випалена земля. Нинішній період історії України він визначав як «постгеноцидний». На його думку, процес інтелектуального і морального занепаду українського суспільства та подальшого зросійщення не змогло зупинити навіть проголошення незалежності. Аж тепер Україна прокинулась – коли спадкоємниця СРСР, Росія, чинить відверту агресію проти української держави, прагнучи стерти її з лиця землі, а нас, українців, втягнути в примарний «русский мир»[15].

Отже, досліджуваний період у правовому регулюванні творчої діяльності в Україні характеризується суттєвим розривом між проголошенням та закріпленням права на свободу творчості на конституційному рівні та можливостями його реалізації. Звинувачення в українському націоналізмі було підґрунтям політичних переслідувань, репресій та знищення творців та науковців. Цензура в УСРР була всеосяжною. Творчість перебувала під жорстким контролем, ідеологічним наглядом.

Отже, щодо обмеження права на свободу творчості на початковому етапі комуністичного будівництва і становлення більшовицького режиму, позиція партійного керівництва була відносно толерантною до українських митців, результатів їх творчості. В той час та території України діяли десятки науково-природничих, технічних і суспільствознавчих мистецьких товариств та творчих об'єднань.

З утвердженням тоталітарного режиму в Україні спостерігається суттєвий розривом між проголошенням та закріпленням права

на свободу творчості на конституційному рівні та можливостями його реалізації. Звинувачення в українському націоналізмі було підґрунтям політичних переслідувань, репресій та знищення творців та науковців. Цензура була всеосяжною. Творчість перебувала під жорстким контролем, ідеологічним наглядом. Багато українських митців були фізично знищені, або морально зламані.

Література:

1. Правова ідеологія і право України на етапі становлення тоталітарного режиму (1929-1941) / Усенко І. Б., МIRONENKO О. М., Чехович В. А. та ін.; За ред. О. М. МIRONENKA, І. Б. Усенка. – К.: Інститут держави і права ім. В. М. Корецького НАН України, 2001. С. 128.
2. Федотова О. Політична цензура в УСРР–УРСР: практика обмеження друкованої продукції. Вісник Книжкової палати. 2012. № 2. С. 45–47.
3. Федотова Оксана. Обмеження друкованого слова в Україні у тридцятих роках ХХ століття. Вісник Книжкової палати. 2009. № 3. С. 32–38.
4. Єжи Гедройць та українська еміграція. Листування 1950–1982 років. Київ: Критика, 2008. 752 с.
5. Програма з «Історії України». Міністерство освіти і науки України, Український державний педагогічний університет імені М.П. Драгоманова; Б.І. Андрусишин, В.Й. Борисенко, М.Л. Головка. Київ: Вид-во ДПУ імені М. П. Драгоманова, 1994. 50 с.
6. Конституция Украинской Социалистической Советской Республики утверждённая Всеукраинским съездом Советов в заседании 10-го марта 1919 года и принятая в окончательной редакции Всеукраинским Центральным Исполнительным Комитетом в заседании 14-го марта 1919 года. 1919. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/CONST28.html. (дата звернення: 15.01.2020).
7. Скуратівський В.Л. Культурна революція. Енциклопедія Сучасної України. Т. 16: «Куз» «Лев» / Гол. редкол.: Дзюба І.М., Жуковський А.І., Железняк М.Г. та ін.; Ін-т енциклопедичних досліджень НАН України. Київ, 2016 URL: http://esu.com.ua/search_articles.php?id=51478 (дата звернення: 12.01.2020)

8. Андрусишин Б. І., Бондаренко В. Д. Формування державно-церковного антагонізму в УРСР у 20-30-х рр. XX ст. Науковий часопис НПУ імені М. П. Драгоманова. Серія № 18. Економіка і право : зб. наукових праць. Випуск 30. К. : Вид-во НПУ імені М. П. Драгоманова, 2015.С. 80-92.

9. Кодекс Законів про народну освіту від 22.11.1922 р. Збірник Узаконовень та Розпоряджень Робітничо-Селянського Уряду України. 1922. 19грудня. Ч.49. - Ст.729.

10. Чорна С. Як Сталін знищував цвіт нації. Голос України. № 146(7152). 19 серпня. 2019 р. С. 8.

11. Конституція Української Соціалістичної Радянської Республіки від 15 травня 1929 р. 33 УРСР. 1929. №14.ст. 100 URL: <https://uk.wikipedia.org/1929> (дата звернення: 08.01.2020).

12. Голод 1932-1933 років на Україні: очима істориків, мовою документів. Упоряд. Р.Я. Пиріг.К.: Політвидав України, 1990. 606 с.

13. Рубльов О., Черченко Ю. Сталінщина й доля західноукраїнської інтелігенції, 20-50-ті роки XX ст.: монографія. Київ: Наук. думка, 1994. С. 16-17.

14. Конституція Української Радянської Соціалістичної Республіки. Вісті ЦВК УРСР від 31 січня 1937 р. №26/4916 URL: <https://uk.wikipedia.org/1929>(дата звернення: 15.01.2020).

15. Овсієнко В. 5 серпня 1937 року. Початок великого терору. Українського інституту національної пам'яті. URL. www.memory.gov.ua (дата звернення: 13.01.2020).

Корж І.Ф.

доктор юридичних наук, старший
науковий співробітник,
завідувач науковою лабораторією
НДІПр НАПр України

ПРАВА І БЕЗПЕКА ЛЮДИНИ В СУЧАСНИХ УМОВАХ

Сучасний, динамічний розвиток інформаційних технологій, особливо цифровізація суспільного життя, ставить гостро на порядок денний питання захисту прав, насамперед інформаційних, та забезпечення безпеки людини. Зазначене викликано тим, що розвиток інтернет-технологій (інформаційно-комунікаційних систем) створює нові можливості для збору, передачі та збереження інформації, що кардинально змінює природу і напрями, механізми і засоби спілкування, метод самовираження людини.

Інтернет, соціальні мережі, електронні реєстри тощо нині стали універсальним механізмом і засобами, джерелами отримання різних відомостей. Кількість користувачів зазначених відомостей невинно зростає, а процес отримання та обміну інформацією стає все більш простішим, швидшим і в значній мірі безкоштовним.

Нині важко собі уявити сучасне життя без Інтернет та соціальних мереж, без гаджетів та інших різноманітних електронних додатків. Зазначене стало невіддільною частиною робочих (службових) процесів, навчання, повсякденного спілкування. Крім того, нині дуже легко можна обмінюватися документами, робочими файлами, фотографіями, влаштовувати конференції, «круглі столи», семінари тощо.

Водночас, сьогодні кожен розуміє, що разом із полегшенням свого життя за допомоги зазначених механізмів і засобів, у людини одночасно виникають проблеми, пов'язані із порушенням прав людини у процесі використання інформаційних технологій, які обумовлені неналежною поведінкою людей, які діють у межах різних юрисдикцій, правової, політичної та інформаційної культури. Цифрова трансформація суспільного життя фактично викликає копіювання не нових, а попередніх моделей поведінки людей. Змі-

нилися лише наслідки такої поведінки та проблеми, пов'язані з її регулюванням.

Таким чином, на сьогодні життя громадян багатьох країн тісно пов'язане із використанням інформаційно-комунікаційних мереж, з іншими електронними гаджетами, і цей зв'язок постійно міцніє і поглиблюється. Людина часто, образно кажучи, «довіряє» цим засобам свої особисті, «потаємні» факти свого життя і надіється на їхнє безпечне там зберігання, недоторканність і цілісність. І ця «співпраця» людини і «електронних засобів», особливо у процесі «цифровізації» суспільного життя, постійно поглиблюється і удосконалюється, одночасно поширюючи і загострюючи конфлікт між ними, який полягає у забезпеченні «недоторканності і цілісності» персональних даних особи. Для прикладу наведемо проблемні питання, пов'язані з такими видами діяльності, як факторинг і колекторна діяльність.

Часто ці два види діяльності часто плутають, тому з'ясуємо сутність цих видів діяльності. Так, колекторська послуга – це діяльність юридичної чи фізичної особи, яка за певну винагороду займається поверненням заборгованості боржника на користь кредитора, тобто фізичної чи юридичної особи, яка має підтверджені належними документами майнові вимоги до боржника (позичальника). Кредиторами можуть бути фізичні особи, юридичні особи (підприємства, організації, установи, урядові структури тощо), держава.

Особливе місце серед кредиторів посідають банки[1]. Банки, які не бажають самостійно вирішувати проблеми неплатежів, звертаються за допомогою до таких компаній. В інших випадках банки можуть створювати спеціальні підрозділи в структурі самого банку або перекладати ці функції на служби внутрішньої безпеки.

В Україні така діяльність законодавчо не врегульована і тісно межує із кримінально карними діями разом з іншими порушеннями законодавства. Однак, у своїй діяльності колектори використовують положення Глави 47 Цивільного кодексу України. Так, відповідно до пункту 1 частини 1 статті 512 ЦКУ, кредитор у зобов'язанні може бути замінений іншою особою внаслідок передання ним своїх прав іншій особі за правочином (відступлення права

вимоги). Отже, з цього випливає, що у разі, якщо банк як кредитор передасть своє право вимоги іншому банку або фінансовій установі (колекторській компанії), це буде достатньою правовою підставою для заміни кредитора в зобов'язанні. З цього моменту всі права та обов'язки, який мав первісний кредитор, переходять до колекторів, зокрема і право фінансової вимоги. За кордоном «колекторська діяльність» (Debt Collection Practice, Debt Collector) законодавчо визначена і врегульована. При цьому метою регулювання є встановлення рамок дозволеного, тобто відповідне законодавство визначає, які дії щодо переконання боржника заплатити є допустимими, а які ні.

Не акцентуючи увагу на багатьох фактах «незаконності» такої діяльності, зазначимо, що колектор може діяти від імені банку (кредитора) на підставі договору доручення, комісії або надання послуг за певну винагороду. В такому випадку банк разом із наданням колектору права вчинити певні юридичні дії щодо стягнення з боржника заборгованості передає колектору інформацію про клієнта-боржника. І саме на цей факт необхідно звернути прискіпливу увагу, оскільки саме в зазначеному криється порушення прав громадян, зміст яких буде розглянуто нижче.

На відміну від колекторських послуг, згідно із законодавством України факторинг належить до фінансових послуг. Здійснювати факторингові операції мають право банки, фінансові установи, приватні підприємці. Сторонами у договорі факторингу є фактор і клієнт. Предметом договору факторингу може бути право грошової вимоги, строк платежу за якою настав (наявна вимога), а також право вимоги, яке виникне в майбутньому (майбутня вимога). Фактор – це банк або інша фінансова установа, яка відповідно до закону має право здійснювати факторингові операції, що передає або зобов'язується передати грошові кошти в розпорядження другої сторони (клієнта) за плату (у будь-який передбачений договором спосіб). Клієнт – це сторона, що відступає або зобов'язується відступити факторові своє право грошової вимоги до третьої особи (боржника), за що отримує від Фактора грошові кошти. Клієнтом у договорі факторингу може бути фізична або юридична особа, яка є суб'єктом підприємницької діяльності.

Діяльність факторингу регулюється положеннями Глави 73 «Факторинг» Цивільного кодексу України [2]. При цьому ст. 1076ЦКУвстановлено, що банк гарантує таємницю банківського рахунку, операцій за рахунком і відомостей про клієнта, тобто його персональні дані, що є банківською таємницею відповідно до ст.60 Закону України «Про банки і банківську діяльність» [3]. Зазначене відповідає положенням Закону України «Про захист персональних даних» [4]. Банки, намагаючись обійти норми ст.62 Закону [3], якими регулюється питання розкриття згаданої таємниці, практикують безпосереднє зазначення в кредитному договорі пункт про передачу інформації про позичальника (з його згоди) третім особам для стягнення заборгованості у випадку її прострочення.

Вирішення зазначеного питання для банків полегшилось після прийняття Закону [5], відповідно до положень якого банки отримали право надавати інформацію, яка містить банківську таємницю, приватним особам та організаціям для забезпечення виконання ними своїх функцій або надання послуг банку відповідно до укладених між такими особами (організаціями) та банком договорів, у тому числі про відступлення права вимоги до клієнта, за умови, що передбачені договорами функції та/або послуги стосуються діяльності банку, яку він здійснює відповідно до статті 47 Закону України «Про банки і банківську діяльність» [3].

Як показує практика, колектори діють також шляхом впливу не тільки на боржника, а й на членів його родини, близьких, співробітників тощо. При цьому необхідною передумовою вчинення такого впливу є наявність інформації про цих осіб, їхні телефони, адреси місця проживання та роботи. Однак, згідно із Законом України «Про інформацію» [6], інформація про особу охороняється законом. А статтею 32 Конституції України визначено, що ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. А отже, збирання, зберігання, використання та поширення особистої інформації про особу без її згоди є прямим порушенням чинного законодавства.

Як показує нинішнє суспільне життя, отримати персональні дані на громадянина не є чимось тяжким. Так 11 травня ц.р. в Телеграм появилася бот, який за гроші поширював персональні дані гро-

мадян України [7], тобто за 20-200 доларів можна навести довідки про паспортні дані, водійські права, банківські реквізити тощо. Бот пропонував знайти людину за ПІБ, за номером телефону, за ідентифікаційним номером платника податку, за адресою електронної пошти і навіть надати паролі від самої електронної пошти [8]. Судячи за кількістю інцидентів, торгівля базами даних з персональною інформацією українців поставлено на потік, тобто інформацією про персональні дані громадян, яку накопичують і зберігають в державних установах і приватних компаніях. Так, в 2017 році податківець із Сум торгував базою даних ДФС. В тому ж році персональні дані клієнтів Приватбанку були скопійовані на російські сервери співробітниками детективної компанії Rroll, яка була найнята Національним банком для пошуку інформації про інсайдерські займи екс-акціонерів банку. У 2018 році в даркнеті продавалася база даних на 18 млн. користувачів «Нової пошти». В тому ж році у Запоріжжі були спіймані продавці даних митниці. У 2019 році був засуджений харківчанин за торгівлю даними ДФС України. Це лише невелика частка інцидентів, які попали в публічну площину.

Згідно першого в історії аудиту держреєстрів, проведеного в 2017 році, в Україні існує більш як 135 держреєстрів. Точна кількість їх невідома, при цьому 80% їх зберігаються локально на сервері держоргану, і лише 60% держреєстрів мають атестовані комплексні системи захисту інформації. Зазначене створює великі ризики у сфері захисту персональних даних громадян. Крім того, зазначене вказує на те, що в Україні немає належного контролю за витоком даних з різних реєстрів персональних даних.

Необхідно зазначити, що в Україні робилися неодноразові спроби врегулювати питання захисту персональних даних громадян за різними напрямками. Так у Верховній Раді України VIII скликання був напрацьований законопроект «Про особливості та заборони здійснення професійної діяльності з врегулювання простроченої заборгованості – колекторської діяльності» [9], тобто своєрідне усунення підґрунтя-діяльності для незаконного пошуку персональних даних. Однак зазначене лишилося лише спробою.

Таким чином перед державою і суспільством залишається невирішеним завдання щодо визначення напрямів і шляхів усунен-

ня зазначених порушень в сучасних умовах, оскільки обмеження чи захист персональних даних людини впливає опосередковано чи прямо на інші права і свободи людини, порушення одного права – викликає порушення іншого. Функціонуючий в Україні Закон [4] явно не справляється зі своїм завданням. Залишається негативним у діяльності щодо повернення заборгованості на сучасному етапі те, що до цього часу відсутня певна законодавча база, що врегулювала б функціонування колекторів. Тому є необхідність в ухвалі відповідних законів, щоб, по-перше, попередити здійснення ряду злочинів, застерегти громадян від дій шахраїв і незаконного втручання в їхнє особисте життя; по-друге, розмежувати на законних підставах повноваження колекторів та інших державних органів, а також визначити міру їх співпраці та невтручання в справи один одного.

В європейських країнах не існує однозначної думки про існування нормативно-правової бази, що пов'язана з поверненням заборгованості, однак всі дії колекторів регламентовані певними нормативно-правовими актами. В Україні заплановані певні кроки у цьому напрямку. Так, запропоновано колекторські фірми перепрофілювати в юридичні компанії. А Національний банк України пропонує своє бачення реформи ринку факторингових (колекторських) послуг. З 1 липня 2010 року планується йому передати контроль за даною сферою, так само як і за страховими компаніями та іншими небанківськими установами [10], що передбачає прозорість структури власності та бездоганну ділову репутацію власників і керівників, а також захищеність прав фізичних осіб-боржників.

Таким чином в умовах сучасності суспільство не повинно відокремлюватися від реального світу, в якому ми зараз живемо. Це суспільство, яке ми будуємо, тому в ньому повинні формуватися такі самі права людини, якими вона наділена у житті. Загалом, вирішення проблем реалізації прав людини в умовах цифрових трансформацій не вбачається можливим без переплетіння взаємодії всіх учасників такого суспільства. Кожен з них повинен бути наділений рівними правами щодо можливостей використання інформаційних технологій, забезпечений вільним та рівним доступом до інформації, мати свободу вираження просторами Інтернету, бути переконаним у тому, що його особисті персональні дані належним

чином будуть захищені, а також мати можливість повністю розпоряджатися своїми персональними даними щодо їх коригування та права бути забутим. Всі ці принципи повинні стати основою для формування цінностей сучасного суспільства.

Список використаної літератури:

1. Кредитор. Вікіпедія. URL:<https://uk.wikipedia.org/wiki/%D0%9A%D1%80%D0%B5%D0%B4%D0%B8%D1%82%D0%BE%D1%80> (дата звернення: 11.05.2020).
2. Цивільний кодекс України від 16.01.2003 р. № 435-IV. *Відомості Верховної Ради України*. 2003. №№ 40-44. Ст. 356.
3. Про банки і банківську діяльність: Закон України від 07.12.2000 р. № 2121-III. *Відомості Верховної Ради України*. 2001. № 5-6. Ст. 30.
4. Про захист персональних даних: Закон України від 01.06.2010 р. № 2297-VI. *Відомості Верховної Ради України*. 2010. № 34. Ст. 481.
5. Про внесення змін до деяких законодавчих актів України щодо врегулювання відносин між кредиторами та споживачами фінансових послуг: Закон України від 22.09.2011 р. № 3795-VI. *Відомості Верховної Ради України*. 2012. № 21. Ст. 197.
6. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. *Відомості Верховної Ради України*. 1992. № 48. Ст. 650.
7. Дія і скандал. Кто виноват в сливе персональных данных миллионов украинцев. URL: <https://ubr.ua/ukraine-and-world/technology/dija-i-skandal-kto-vinoven-v-slive-personalnykh-dannykh-millionov-ukraintsev-3892756>. (дата звернення: 13.05.2020).
8. Держреєстри потекли: хто «зливає» персональні дані українців і що з цим робити. URL:<https://www.epravda.com.ua/publications/2020/05/13/660405/> (дата звернення: 13.05.2020).
9. Про особливості та заборони здійснення професійної діяльності з врегулювання простроченої заборгованості – колекторської діяльності: проект Закону від 17.05.2017 р. № 6417-2. URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=61806. (дата звернення: 13.05.2020).
10. НБУ перекроєт ринок колекторських услуг – готує реформу. URL:<https://ubr.ua/finances/finance-ukraine/nbu-perekroit-rynok-kollektorskich-usluh-hotovit-reformu-3892672> (дата звернення: 13.05.2020).

Золотар О.О.,

доктор юридичних наук, старший науковий співробітник,
Науково-дослідний інститут інформатики і права Національної академії правових наук України

БЕЗПЕКА І ПРАВА ДИТИНИ В ЧАСИ ПАНДЕМІЇ (НА ПРИКЛАДІ ФРАНЦІЇ)

Глобальна пандемія, окрім безпосередньої загрози захворювання на коронавірус Covid-19, актуалізувала низку інших загроз для суспільства – економічні збитки; зростання безробіття; соціальні ізоляція і, як наслідок, криза довіри; труднощі у доступі до медичної допомоги у зв'язку з загальними і хронічними хворобами; інші обмеження прав людини, які подекуди стали втручанням держави в особистий простір людей.

Генеральний директор Всесвітньої організації охорони здоров'я Тедрос Адханом Гебрейесус зазначив, що «соціальна ізоляція, страх інфікування і втрати членів сім'ї поглиблюються стресом, викликаним втратою доходів, а нерідко і місця роботи. Дані, що надходять вже вказують на поширення симптомів депресії і тривожних розладів серед населення цілої низки країн».[1]

Діти і підлітки становлять особливу групу ризику, з огляду на несформованість психіки, залежність від дорослих, а в умовах карантину – ще й соціальну ізоляцію, що складно переживається в юному віці. В Італії та Іспанії батьки скаржаться на те, що у їхніх дітей виникають труднощі з концентрацією уваги, а також підвищена дратівливість і нервозність. Введення режиму самоізоляції збільшило ризик епізодів насильства або жорстокого поводження по відношенню до дітей або в їх присутності.

У країнах ЄС, де карантин запровадили раніше, ніж в Україні, зокрема, у Франції ще в березні зафіксували зростання домашнього насильства, а кількість звернень зросла на 30% [2]. В квітні глава ООН Антоніо Гутеррес повідомляв про “жахливий глобальний сплеск домашнього насильства, пов'язаний з обмеженнями, вве-

деними урядами у відповідь на пандемію COVID-19»[3]. В Україні подібної статистики просто немає, але це не означає, що немає проблеми.

З досвіду Франції можна звернути увагу на документ «Прислухатись до висловлювань учнів після повернення з карантину у зв'язку COVID 19»[4]. Ця рекомендація Міністерства освіти Франції звертає увагу, що у період поступового відновлення навчального процесу, місією школи є подолання ситуації, що виникла внаслідок пандемії, забезпечення підтримки учнів та співробітників, щоб осмислити цю дійсність та дозволити відновити функціонування навчальної спільноти. Несподіване і безпрецедентне поширення COVID-19 стало джерелом сильних емоцій, а іноді ірраціональних реакцій...». Це документ вказує на ризик щодо неправильного тлумачення ідеї “повернення до нормального життя” та необхідність пильності щодо поняття “повернення”. Щоб створити умови для осмислення дійсності пропонується надати учням можливість висловлюватись щодо ситуації, яка склалась. Зокрема, для підтримки таких дискусій необхідні два взаємодоповнюючих підходи:

«1. Після кризи повернення до попереднього життя “як раніше” є неможливим, тому виникає питання переосмислення життя, зокрема, шкільного. Цей перехідний момент вимагає зусиль для (пере)будови і обов'язково призведе до вдосконалення та трансформації. Не виключено, що необхідні дуже специфічні умови для відновлення навчання в школі.

2. Школа, покликана бути безпечним місцем для життя, яке дозволяє учням знайти (віднайти) «мирне повсякденне життя»[4].

Таким чином, можна зробити висновок про акцент на можливість дитини самовиражатись і знаходити підтримку в шкільному середовищі, що особливо важливо з огляду на тривалу ізоляцію, збільшення кількості випадків домашнього насилля, а також вразливість дітей до стресових станів. Водночас, наполягання на необхідності переосмислення категорії «мирного повсякденного життя» насторожує. Адже таким чином зачіпається сфера «смислів» дитини - її ціннісних установок, адаптивності до змін та лояльності до певних соціальних процесів. При формуванні смислів відбувається «робота з інтерпретаціями, виходячи з наявної моделі світу,

а факти можуть зазнавати змін на рівні інтерпретацій» [5]. Радзієвська О.Г. безспідставно стверджує, що «інформаційне середовище, що оточує дитину має значний вплив на формування її особистості. При відсутності, або недостатній кількості інших комунікаційних зв'язків та позитивних (кореляційних) інформаційних впливів авторитетних для дитини осіб, її внутрішній світ формується з ілюзорних, створених штучно образів, які підмінюють справжні цінності та спотворюють, викривляють погляди дитини» [6].

З огляду на вбєсазначене, хочу звернути увагу на ще один документ Міністерства освіти Франції – «Covid 19 та ризик сектанських аберацій» [7]. В ньому зазначається, що криза Covid-19 послабила психічну стійкість населення та сприяє розвитку почуття вразливості. Виняткова ситуація та експлуатація страхів та страждань, які вона породжує, сприятливі для ризиків сектантських аберацій та посилення прихильності послідовників. Починаючи з 17 березня 2020 року, дати, коли французький уряд ввів карантинні заходи, MIVILUDES²отримала значну кількість повідомлень про негативний вплив сект на дітей. І з метою запобігання та припиненню такого впливу визначено необхідність:

- 1) ідентифікувати зміни в поведінці учнів через вплив сім'ї і зовнішніх чинників;
- 2) попередити ризик дестабілізації учнів і їх ірраціональної поведінки
- 3) поінформувати учнів про ризики небезпечних промов, які дають неправдиві слова про засоби захисту та небезпечні поради щодо COVID-19;

² MIVILUDES – французьке скорочення від Mission interministérielle de budigence et de lutte contre les dérives sectaires, дослівно - Міжвідомча місія пильності та боротьби з сектантськими абераціями, французька урядова установа, до чїїх завдань належить: спостереження та аналіз явищ сектантських рухів, чїї практики завдають шкоди правам людини та основним свободам, становлять загрозу для громадського порядку або суперечать чинним законам та нормам; координація превентивних та репресивних дій з боку влади проти такої практики; розвиток обміну інформацією між державними службами про адміністративні практики, пов'язані з боротьбою з сектантськими абераціями; сприяння інформуванню та навчанню державних агентів у цій галузі; інформування громадськості про ризики та, в деяких випадках, небезпеки, що виникають внаслідок сектантських відхилень, та сприяння здійсненню дій з надання допомоги жертвам такої практики; участь у заходах, що стосуються питань, що належать до її сфери, здійснює на міжнародному рівні Міністерство закордонних справ.

4) розвинути критичне мислення в учнів задля кращого протистояння дезінформації, неправдивим новинам, чуткам та теоріям змови [4].

На перший погляд, дуже обґрунтовані і позитивні наміри. Проте, зміст документу далі як основні загрози ідентифікує діяльність «деяких проповідників, гуру або ідеологів, які трактують ситуацію як: волю і могутність Божу; бунт природи, сил темряви або божественних духів; кару, послана Богом і апокаліптичні знаки; а також повернення до віри як до єдиної можливості спасіння»[4]. Під такий опис легко підвести вчення навіть основних світових релігій (християнства, ісламу, юдаїзму).

Крім того, при поновленні навчання в школі вчителів та інший шкільний персонал зобов'язали звертати увагу на зміни в поведінці учнів, збирати факти на основі адаптованих питань з метою запобігання та боротьби з ризиками сектантської деривації. «В разі виявлення впливу сект, весь персонал зобов'язаний попередити відповідні служби для того, щоб захистити фізичну та моральну недоторканність неповнолітнього» [4].

Насторожує, що такий документ має дуже тонку межу між забезпечення інформаційно-психологічної безпеки дитини і втручанням в особисте життя її сім'ї, а навіть порушення права на свободу думки, совісті і релігії, яке так само передбачено як для дорослих, так і для дитини(ст.14 Конвенції про права дитини[8]). В той же час, норма згідно Декларації про ліквідацію всіх форм нетерпимості та дискримінації на підставі релігії чи переконань, «батьки або, у визначених випадках, законні опікуни дитини, мають право визначати спосіб життя в сім'ї у відповідності зі своєю релігією або переконаннями, а також виходячи з морального виховання, яке, на їхню думку, повинна отримати дитина.» (ч. 1 ст. 5)[9].

Джерела:

1. Substantial investment needed to avert mental health crisis. 14 May 2020. URL:<https://www.who.int/ru/news-room/detail/14-05-2020-substantial-investment-needed-to-avert-mental-health-crisis>
2. Domestic violence cases jump 30% during lockdown in France. 28/03/2020. URL: <https://www.euronews.com/2020/03/28/domestic-violence-cases-jump-30-during-lockdown-in-france>

3. UN chief calls for domestic violence 'ceasefire' amid 'horrifying global surge'. 6 April 2020. URL: <https://news.un.org/en/story/2020/04/1061052>

4. Ecouter la parole des élèves en retour de confinement COVID 19. URL: https://cache.media.eduscol.education.fr/file/Reprise_deconfinement_Mai2020/69/3/Fiche-Ecouter-favoriser-parole-des-eleves_1280693.pdf

5. Почепцов Г. Смисли і війни: Україна і Росія в інформаційній і смисловій війнах. Видавничий дім «Києво-Могилянська академія» 2016 р. 316 с.

6. Радзівська О. Г. Проблеми захисту прав і безпеки дитини в інформаційній сфері: монографія, за заг. ред. В.Г. Пилипчука. К.: Видавничий дім «АртЕк». 2019. 238 с.

7. Covid 19 et risques de dérives sectaires. URL: https://cache.media.eduscol.education.fr/file/Reprise_deconfinement_Mai2020/69/2/Fiche-Derives-sectaires_1280692.pdf

8. Конвенція про права дитини від 20 листопада 1989 р. URL: https://zakon.rada.gov.ua/laws/show/995_021

9. Декларація про ліквідацію всіх форм нетерпимості та дискримінації на підставі релігії чи переконань від 25 листопада 1981 р. URL: https://zakon.rada.gov.ua/laws/show/995_284

Гордієнко С.Г.

доктор юридичних наук, доцент
завідувач кафедри національної безпеки
навчально-наукового інституту права
ім. князя Володимира Великого МАУП

СТАН І ПЕРСПЕКТИВИ ВИВЧЕННЯ ТА АНАЛІЗУ ПРАВОВИХ АСПЕКТІВ ЖИТТЄВОГО ЦИКЛУ ІНФОРМАЦІЇ

Слід зазначити, що винесена організаторами конференції для обговорення тема стосовно захисту прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах розвитку державності є вкрай актуальною. Адже суспільство засноване на знаннях, а тим більше на якісно нових знаннях, створених у ході інноваційної діяльності має бути захищеним від їх, у тому числі, небезпечного впливу.

Всім відомо, що зміїна отрута у великій кількості смертельна для людини, а в малих дозах – ліки! Так і інформаційні ресурси, у безмежній кількості, а тим більше некласифіковані, призводять непідготовленого слухача та читача у панічний стан і розпач, а коли людині відомі механізми створення, розповсюдження та захисту інформації вона чітко розуміє де корисна інформація, а де фейки, а тим більше дезінформація.

Зазначене питання цікавить автора вже майже 25 років і перші кроки, і сподівання вивчити зазначену проблему і проаналізувавши реальний стан питання навести вичерпні відповіді не дали бажаного швидкого результату. Та навіть за такий проміжок часу відчувається величезна складність при вивченні т.з. інформаційної сфери.

Суть зазначеної проблеми лежить в філософській, тобто загально-науковій невизначеності основної маси понять, що застосовуються, відсутності класифікації інформаційних ресурсів, їх життєвого циклу і взаємопереходів, відсутності відповідних методик визначення їх грошової цінності, а також відповідно до їх ціни методик захисту та впливу на людину.

Відповідно до зазначеного вище автором зроблена спроба відповісти на ряд визначених вище питань у своїх роботах. Основними з них були теоретико-прикладні питання відповідно до трьох

сфер: створення, використання та захисту інформаційних ресурсів; природи та змісту інноваційної діяльності; та права на інтелектуальну власність.

Автор впевнений, що діяльність науковців за даним напрямом буде приречена на невдачу, бо без вирішення фундаментальних теоретичних питань приречена на невдачу робота над «загрозами кіберцивілізації із штучним інтелектом».

Тобто, при спробі розгляду зазначених питань автору довелося розглянути філософські аспекти проблематики і відпрацювати «правила» визначення понять і застосувати їх потенціал у відзначених сферах і частково йому це без сумніву вдалося.

Таким чином було ґрунтовно розглянуто та досліджено:

1. Теоретико-прикладні питання сфери створення, використання та захисту інформаційних ресурсів:

- понятійно-категоріальний апарат сфери інформаційного права, як системоутворюючий аспект її регулювання;
- алгоритм створення і життєвого циклу інформаційних ресурсів та проблеми їх захисту;
- доктринальні положення інформаційної безпеки України;
- реалії та перспективи забезпечення інформаційної безпеки держави та завдання державних та недержавних структур із захисту інформації з обмеженим доступом та їх нормативно-правове регулювання в Україні в сучасних умовах;
- нормативне забезпечення окремо виділених складових інформаційної сфери держави;
- теоретичні та прикладні основи оцінювання інформаційних ресурсів;
- співвідношення права на інформацію та права на інтелектуальну власність;
- питання фундаментальності підготовки молодих юристів, як необхідної умови розуміння проблем захисту інформації з обмеженнями у доступі та інтелектуальної власності в Україні;
- зміст навчальних програм науково-навчального предмету «інформаційне право»;
- схожість та відмінності понять та діяльності – «шпигунство, промислове шпигунство та бізнес-розвідка»;

- концептуальні засади антирозвідувальної діяльності на підприємствах і розроблена технологія протидії конкурентній розвідці.

2. Теоретико-прикладні питання сфери інноваційної діяльності:

- основні поняття сфери інноваційної діяльності як системоутворюючі аспекти її регулювання;
- сутність, зміст та джерела інноваційної діяльності в Україні під кутом протиріч теорії та практики;
- сукупність та значення державних органів та недержавних структур і їх компетенцію в інноваційній політиці та науково-технічній діяльності;
- напрями удосконалення державної політики з урахуванням змісту загроз інноваційній діяльності;
- концептуальні засади науково-навчального предмету «інноваційна діяльність».

3. Теоретико-прикладні питання права на інтелектуальну власність:

- понятійний апарат стосовно «інтелектуальної власності» та класифікація сфер творчості людини як системоутворюючі аспекти їх регулювання;
- співвідношення інформаційного права та права на інтелектуальну власність;
- проблеми в захисті інтелектуальної власності в Україні;
- загрози інформації з обмеженнями та інтелектуальній власності, як загрози існування державності та напрями їх нейтралізації;
- алгоритм кодифікації законодавства з питань інтелектуальної власності;
- теорію та практику розвитку людського капіталу в Україні;
- забезпечення захисту інтелектуальної власності як пріоритетний науковий напрямок та навчальне завдання системи освіти України;
- необхідність фундаментальної підготовки молодих фахівців, як умови розуміння проблем захисту інформації з обмеженнями у доступі та інтелектуальної власності в Україні;
- створення і життєвий цикл інтелектуального продукту як основи єдиного навчального та наукового напряму – «інтелектуальна власність»;

- значення юридичної науки в процесі виховання інженерно-технічних кадрів;
- негативну роль чиновництва України в сфері захисту інтелектуальної власності.

Результати роботи за даним напрямом автором відображені у 7-и монографіях, 3-х посібниках, 30-и статтях, 40-а тезах на наукових форумах, 7-и курсах лекцій, 20 публікаціях у науково-популярних виданнях, однак вони не були об'єднані єдиним задумом тому і не знаходили свого цілісного відображення. Це стало приводом до перегляду та систематизації авторської позиції, що вилилася у чернетку посібника «Інформація – інновації – інтелектуальна власність та її захист в Україні: теоретико-прикладні проблеми».

Звичайно, автор не претендує на істинність за даними питаннями, а тому вже неодноразово наполягав на створенні творчого колективу для дослідження зазначеної тріади під егідою НДПП, НДПВ та НДПЗІР Національної академії правових наук України.

Адже виступи фахівців на таких знакових конференціях у провідних наукових та навчальних закладах як:

- Інформаційне право: сучасні виклики і напрями розвитку;
- Інформаційні правовідносини як інститут приватного права;
- Права, свободи і безпека людини в інформаційній сфері;
- Теоретико-правові основи формування та розвитку інформаційного суспільства - «суспільства знань»;
- Правове регулювання інформаційних відносин та управління інформаційною безпекою держави;
- Правове регулювання суспільних відносин в умовах демократизації;
- Охорона прав інтелектуальної власності в Україні та Європейському Союзі: політика, законодавство, практика;
- Інтелектуальна власність і право на шляху до сталого розвитку України;
- Право інтелектуальної власності та охорона прав інтелектуальної власності в Україні;
- Право інтелектуальної власності та охорона прав інтелектуальної власності в Європейському Союзі;
- Право інтелектуальної власності як інститут приватного права;

- Проблеми підготовки фахівців з інтелектуальної власності, інформаційно-аналітичної та інноваційної діяльності в Україні;
- Використання результатів наукових досліджень та об'єктів інтелектуальної власності;
- Правове регулювання сфери інтелектуальної власності в умовах кіберцивілізації;
- Стан та перспективи самореалізації людини в Україні;
- Правові питання трансформації інформаційного суспільства в суспільство знань, як основи інноваційного розвитку України та багатьох інших наукових форумах (Київ, Запоріжжя, Одеса, Дніпро та Луцьк), і інші вагомі здобутки потребують скрупульозного вивчення та узагальнення за чітко визначеними та затвердженими напрямками.

Останнє, на глибоке переконання автора, призведе до розробки науково-виважених, життєздатних на практиці доктрин, концепцій, стратегій та програм галузей державної діяльності з інформаційного права, інноваційної діяльності та права на інтелектуальну власність.

Солодка О.М.

кандидат юридичних наук, старший
науковий співробітник
докторант Національної академії
Служби безпеки України

СВОБОДА ІНФОРМАЦІЇ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОГО СУВЕРЕНІТЕТУ УКРАЇНИ

У період інформаційного суспільства особливістю основних загальноцивілізаційних процесів є раніше невідома активізація двох діалектично пов'язаних тенденцій: необмежені можливості у доступі до інформації та їх використання у протиправних цілях. В зазначених умовах держава відчуває нагальну потребу у забезпеченні інформаційної безпеки, що неможливо реалізувати за відсутності інформаційного суверенітету. Хоча остання категорія здебільшого негативно сприймається представниками ліберальних режимів як така, що суперечить теорії свободи інформації та зводиться до контролю за інформаційними потоками.

Свобода інформації – поняття, що використовується для позначення групи прав і свобод людини, включаючи право на інформацію (право вільно збирати, зберігати, використовувати і поширювати інформацію), свободу вираження поглядів і переконань, свободу думки і слова, свободу обміну інформацією.

Концепція свободи інформації була вперше запропонована на міжамериканській конференції 1945 р. у Мехіко як свобода шукати, отримувати та поширювати інформацію будь-якими засобами й незалежно від державних кордонів. У 1946 р. свобода інформації як фундаментальне право людини було проголошено на першій сесії Генеральної асамблеї ООН у Резолюції 59 (I) “Скликання міжнародної конференції з питань свободи інформації”. Згодом ця концепція знайшла своє втілення в Загальній декларації з прав людини, Міжнародному пакті про громадянські та політичні права та інших міжнародних документах, що стосуються прав і свобод людини і громадянина. Зокрема, у резолюції 59 (1) Генеральної Асамблеї ООН зазначено, що “свобода інформації є основним правом людини і критерієм усіх інших свобод”.

Гарантії інформаційних прав і свобод людини належать до найважливіших засад формування правової держави та громадянського суспільства. Ці права включені і до дієвого механізму державного управління в демократичному суспільстві, що визначає забезпечення захисту прав і свобод людини в інформаційній сфері однією з найважливіших цілей інформаційної безпеки, а власне людину – найголовнішим її об'єктом.

Право на свободу інформації гарантується Конституцією України, що закріплено в наступних положеннях:

- гарантія права на свободу думки і слова, на вільне вираження своїх поглядів і переконань (частина 1 ст. 34);
- право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір (частина 2 ст. 34);
- гарантія права вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення. (частина 2 ст. 50) [1].

Суверенітет – це верховенство влади всередині країни та її незалежність і рівноправність у зовнішніх зносинах. Поняття інформаційного суверенітету держави відображає верховенство державної влади в національному інформаційному просторі та рівноправність у міжнародних відносинах в глобальному інформаційному просторі. Зазначене реалізується відповідно до законодавства України та норм міжнародного права через самостійне і незалежне визначення та здійснення державної внутрішньої і зовнішньої інформаційної політики з метою забезпечення національних інтересів України в інформаційній сфері та протидії інформаційним загрозам.

Саме підвищення ролі інформації в суспільстві, зростання її обсягів, стрімкий розвиток інформаційних відносин та їх перенесення в цифровий вимір вимагає від кожної держави приділяти значну увагу захисту свого інформаційного простору, що реалізується власне через концепцію інформаційного суверенітету. Загалом підходи до її розуміння різняться залежно від політичного режиму, рівня розвитку інформаційних технологій, реальних та потенційних загроз в інформаційній сфері, проте саме свобода інформації є її невід'ємним критерієм.

Суттєвим аспектом свободи інформації у співвідношенні з інформаційним суверенітетом є двоєдина концепція, що лежить в основі цього права, основними елементами якої є “свобода доступу до держави” і “свобода від держави”. Соціалістична концепція передбачає ж розглядати свободу як певний припис, вказівку або “директиву, що прописує свободу, спрямовану не стільки на попередження втручання держави в особисте життя індивідуума, скільки на його соціальну інтеграцію у суспільне життя” [2].

“Свобода від держави” реалізується через гарантії права людини на невтручання в особисте життя. Зокрема, в ст. 32 Конституції визначено: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини». Ст. 31 Конституції України гарантує кожному таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинів чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо [1]. Надалі ці положення знаходять своє відображення в інституті захисту персональних даних.

«Свобода доступу до держави» основним чином реалізується через доступ до інформації, який у суб'єктивному розумінні визначається як гарантована державою можливість фізичних, юридичних осіб і держави (державних органів) вільно одержувати відомості, необхідні їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій, що не порушує права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. В об'єктивному розумінні доступ до інформації – це сукупність правових норм, що регламентують суспільні інформаційні відносини щодо одержання їх учасниками відомостей, необхідних їм для реалізації своїх прав, свобод і законних інтересів, здійснення завдань і функцій [3].

Інформація є з'єднуючою ланкою між людиною і суспільством. Достовірне і вчасне інформування громадян з боку держави та на-

дання необхідної для функціонування держави інформації з боку громадян є запорукою формування дійсно громадянського суспільства, розбудови демократичної і правової держави. В означеному контексті з правом інформаційної свободи, яке апіорі передбачає всю інформацію як загальнодоступну, пересікається інститут інформації з обмеженим доступом. Відсутність чітких критеріїв віднесення інформації до категорії з обмеженим доступом, а також конкретної процедури обмеження доступу до неї сприяють зловживанням органами державної влади шляхом ненадання інформації через неправомірне застосування грифів обмеження доступу до інформації.

Демократичне суспільство ж ґрунтується не на вільному балансі між свободою та соціальною справедливістю, свободою та державним інтересом. Межі свободи можуть бути визначені тільки правовим законом, який і є її мірою [4].

Свобода інформації може бути обмежена для дотримання інших прав особистості (таємниця зв'язку, кореспонденції, захист від втручання в особисте та сімейне життя), так і для захисту інтересів суспільства (обмеження в період дії надзвичайного або воєнного стану).

Частина 3 статті 34 Конституції України формулює виключний перелік підстав для обмеження права на інформацію: в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя [1].

В даному випадку мова йде про дотримання двох принципів. Перший – принцип максимального оприлюднення: вся інформація, яку зберігають державні органи влади, підлягає оприлюдненню, винятки можуть бути тільки для дуже обмеженого числа випадків. Другий принцип характеризує вимоги щодо обмежень: а) винятки повинні бути зрозумілими, б) описуватися вузько, в) підлягати контролю на предмет наявності «шкоди» і впливу на «суспільні інтереси» [5].

Відтак, еволюція свободи інформації в теоріях інформаційного суспільства розглядається без урахування обмежень: в них затверджуються ідеї свободи, але більшою мірою ігноруються принципи інформаційної безпеки. Таким чином, свобода інформації повинна бути основою інформаційних відносин, гарантом прозорості та законності діяльності державної влади, проте регулювання суспільних інформаційних відносин повинно мати на меті створення сприятливих для умов для як доступу до інформації, так і забезпечення інформаційної безпеки.

З урахуванням зазначеного основоположними началами забезпечення інформаційного суверенітету держави є: презумпція інформаційної свободи як базис реалізації інформаційного суверенітету; захищеність інформаційної приватності людини; забезпечення права на інформацію як обов'язок держави.

Реалізація інформаційного суверенітету держави передбачає забезпечення прав і свобод людини в інформаційній сфері; визначення виключних підстав для обмежень, що встановлюються при забезпеченні інформаційного суверенітету держави; пошук балансу між правами людини і необхідністю реалізації цілей держави в інформаційній сфері.

Література

1. Конституція України: Закон України від 28.06.96 р. Відомості Верховної Ради України. 1996. № 30. Ст.141.
2. Резолюция Комиссии по правам человека. Поощрение и защита права на свободу убеждений и их свободное выражение. Доклад Специального докладчика г-на Абида Хуссейна, подготовленный в соответствии с резолюцией 1993/45 Комиссии по правам человека. 19 декабря 1994 г. E/CN.4/1995/32. URL: <http://www.daccess-ods.un.org/TMP/7821679.71134186.html>. (дата звернення 15.05.2020).
3. Марущак А.І. Визначення поняття “доступ до інформації”. Правова інформатика. № 3 (11)/2006. с.69-74.
4. Юридична енциклопедія: в 6 т. / Редкол.: Шемшученко Ю.С. (відп. ред.) та ін. – К.: “Укр. енцикл.”, 2003. Т 5. – 736 с.
5. Принципи законодавства про свободу інформації. Стаття 19. Лондон, червень 1999. URL: <http://www.khpg.org/index.php?id=968017351> (дата звернення 01.03.2020).

Белевцева В.В.

доктор юридичних наук, старший науковий співробітник, завідувач науково-дослідної лабораторії правових проблем та відповідальності у сфері цифровізації НДІ інформатики і права

ПРАВОВІ ЗАСАДИ МЕХАНІЗМУ ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД ЛЮДИНИ В УКРАЇНІ

На сучасному етапі розвитку світової спільноти проблеми захисту прав людини виходять далеко за межі окремої держави. Сформувалися та отримали загальне визнання міжнародні норми і принципи у сфері прав людини, що є стандартом, до досягнення якого повинні прагнути усі держави. Ці норми і принципи містяться у найважливіших міжнародно-правових документах з питань захисту прав людини. Загальній Декларації прав людини (1948 р.), Міжнародному пакті про цивільні і політичні права (1966 р.), Міжнародний пакт про соціально- економічні і культурні права (1966 р.), Факультативному протоколі до Міжнародного пакту про цивільні і політичні права (1966 р.), що склали Міжнародний білль про права людини. На регіональному рівні ці норм містяться у Європейській Конвенції про захист прав людини і основних свобод (1950 р.), Європейську соціальну хартію (1961 р.). Більшість цих документів носять юридично обов'язковий характер для держав, які їх ратифікували.

Проблема захисту інформаційних прав, встановлення чіткого механізму їх реалізації актуальна й сьогодні тим, що за його допомогою вони знаходять дієвість і реальність, забезпечуючи тим самим їх, маючи можливість задовольняти інтереси у різних сферах життєдіяльності людини. Дослідження особливостей механізму захисту інформаційних прав дозволяє виявити ключові проблеми в реалізації правових норм, регулюючих відповідні суспільні стосунки, та розробити нові шляхи удосконалення чинного законодавства з питань пошуку, здобуття, передачі, створення і поширення інформації.

Розгляд основ правового статусу особи дозволяє виділити ідею, відповідно до якої зафіксовані в українській Конституції інформаційні права утворюють чітку і послідовну систему. Свобода думки, слова, масовій інформації і право на доступ до інформації органів влади гарантують можливості громадян відповідно мати переконання і не піддаватися у зв'язку з цим дискримінація, висловлювати свої думки і робити їх відомими, відстоювати свої ідеї та впливати на їх облік владою, нарешті, контролювати владу - наскільки дані ідеї враховані.

Концептуальні підстави системи захисту інформаційних прав і свобод людини і громадянина, маючи історичну обумовленість і отримуючи відповідне конституційне закріплення, забезпечують її необхідні спадкоємність, стабільність і динаміку. В Україні відмічається принципова зміна пріоритетів на користь людини, його прав і свобод, що знаменує становлення демократичної концепції захисту прав і свобод людини і громадянина. Стабільність і життєздатність останньою тісно пов'язана, на нашу думку, з розширенням її соціально-регулятивних засад [1].

Підвищення ефективності реалізації правового механізму захисту інформаційних прав і свобод людини і громадянина в Україні у ряді випадків можна досягти за допомогою перерозподілу правозахисної компетенції між деякими державними органами.

Якісне перетворення і реальне удосконалення захисту інформаційних прав і свобод людини і громадянина в Україні можливе за умов виявлення закономірностей його функціонування, тенденцій розвитку, неблагополучних, з правозахисної точки зору, елементів державного механізму. Забезпечення наведених умов зв'язується з систематичною, глибокою аналітичною роботою, об'єктивні результати якої дозволять органам, наділеним владними повноваженнями приймати відповідні рішення, комплексні правозахисні заходи щодо інформаційних прав і свобод людини [1].

Зміцненню в Україні цілісного механізму захисту прав і свобод людини, такого, що відповідає новітнім викликам і загрозам інформаційній безпеці перешкоджають наступні чинники, які склалися на практиці, зокрема: корпоративний опір носіїв влади незалежній правозахисній діяльності, проблеми свободи ЗМІ, відсутність на-

лежного рівня правової інформованості в суспільстві і неконструктивне суперництво між суб'єктами правозахисної діяльності, що мають єдину або різну правову природу. Подолання деструкції такої конкуренції - найбільш складно вирішуване завдання, оскільки цього не можна досягти простим велінням [3].

Аналіз положень чинного законодавства України дає можливість стверджувати, що існуючі права та обов'язки людини і громадянина у сфері інформації доцільно вважати за особливу групу прав – інформаційними правами, що включають: право на вільний пошук інформації, право на передачу інформації, право отримувати інформацію, право на виробництво інформації, право на розповсюдження інформації тощо [1; 2; 3].

Також виявлено два шляхи виникнення інформаційних прав і свобод людини і громадянина у правовій системі української держави [1]:

- 1) шляхом ухвалення нових нормативно-правових актів внутрішньо державного характеру, що закріплюють нові інформаційні права людини і громадянина;
- 2) шляхом ратифікації міжнародних угод, що містять нові інформаційні права людини і громадянина.

Дослідження законодавства України з питань забезпечення інформаційної сфери дозволило виявити існування такого правового явища, як правовий механізм захисту інформаційних прав і свобод людини і громадянина, що є різновидом механізму захисту прав і свобод людини і громадянина у цілому.

Правовий механізм захисту інформаційних прав і свобод людини і громадянина поділяється на нормативно-правовий та організаційно-правовий.

Нормативно-правова форма виражається в ухваленні нормативно-правових актів або у внесенні до існуючих нормативно-правових актів таких змін, які можуть сприяти здійсненню захисту інформаційних прав людини і громадянина.

Натомість організаційно-правова форма виражається в діяльності державних органів, що беруть участь у процесі захисту прав інформаційної людини і громадянина на території України.

У результаті детального розгляду нормативно-правового механізму захисту інформаційних прав і свобод людини і громадянина

в Україні були виявлені наступні його елементи: нормативне закріплення здійснення правового захисту інформаційних прав людини і громадянина; юридичний факт, який дозволяє почати процес правового захисту інформаційних прав людини і громадянина; правовідносини, в яких є права та відповідні ним обов'язки; суб'єкти правового механізму захисту інформаційних прав людини і громадянина; об'єкти правового механізму захисту інформаційних прав людини і громадянина [1].

На основі аналізу елементів нормативно-правового механізму захисту інформаційних прав і свобод людини і громадянина виявлені його особливості як правового явища, які полягають в унікальності інформаційної сфери, в якій реалізується цей механізм, а також предметів (об'єктів), з приводу яких, виникають відповідні правовідносини (інформація та її носії).

Слід наголосити, що нормативно-правовий механізм захисту інформаційних прав людини і громадянина є частиною правового механізму захисту усіх конституційних прав і обов'язків. Одним з найважливіших компонентів правового механізму захисту інформаційних прав людини і громадянина в Україні є їх гарантії. Зміст правових гарантій інформаційних прав і свобод людини і громадянина, закріплених в міжнародно-правових актах та у національному праві є практично ідентичним. Проте підстави їх можливого обмеження та прямі обмеження, визначені в міжнародних документах та вітчизняному законодавстві не завжди збігаються. У зв'язку з цим, пропонуємо провести уніфікацію переліку підстав для обмежень інформаційних прав і свобод людини і громадянина та створити перелік випадків їх прямого обмеження з подальшим закріпленням в законодавстві.

Необхідно відзначити особливості нормативно-правового механізму захисту інформаційних прав і свобод людини і громадянина. Такими особливостями є принципи гарантованість права на інформацію; відкритість, доступність інформації, свобода обміну інформацією; достовірність і повнота інформації; свобода вираження поглядів і переконань; правомірність одержання, використання, поширення, зберігання та захисту інформації; захищеність особи від втручання в її особисте та сімейне життя [2].

Дослідивши, у свою чергу, організаційно-правовий механізм захисту інформаційних прав і свобод людини і громадянина в Україні можна дійти висновку, що основна роль у ньому належить Президентові України, Верховній Раді України, органам виконавчої влади, правоохоронним органам, а також інститутам громадського суспільства [3]. Роль Президента України в організаційно-правовому механізмі захисту інформаційних прав і свобод людини і громадянина в Україні обумовлена тим, що він є гарантом прав і свобод людини в українській державі [3]. Роль органів виконавчої влади в організаційно-правовому механізмі захисту інформаційних прав і свобод людини і громадянина виражається в організації виконання норм Конституції України і законів, також вона реалізується через аналітичну роботу [3]. Особливе місце в організаційно-правовому механізмі захисту інформаційних прав і свобод людини і громадянина відводиться правоохоронним органам (судам, прокуратурі, органам МВС, адвокатурі, нотаріату), які відіграють найактивнішу роль у захисті інформаційних прав і свобод людини і громадянина. Таке положення обумовлене самою правовою природою і функціями вказаних органів.

Отже, глибокий системний аналіз правового механізму захисту інформаційних прав і свобод людини і громадянина в Україні дозволив сформулювати пропозиції щодо подальшого його удосконалення та підвищення ефективності.

Тобто, по-перше, пропонується ухвалити закон, що регулюватиме умови і порядок реалізації права на інформацію, що, у свою чергу, дозволить скоротити об'єм підзаконного правового регулювання.

По-друге, пропонуємо створити спеціалізовані суди, діяльність яких буде пов'язана із захистом інформаційних прав і свобод людини і громадянина (інформаційних судів).

У підсумку зазначимо, що теоретичне осмислення дії правового механізму захисту інформаційних прав і свобод людини і громадянина необхідне тому, що в цьому питанні не можна обійтися лише аналізом і коментуванням чинного законодавства в інформаційній сфері. Необхідне системне теоретико-правове обґрунтування і дослідження цієї найважливішої правової проблеми.

Список використаної література

1. Белевцева В.В. Правовий захист інформаційних прав і свобод людини і громадянина в Україні: проблеми та перспективи / В.В. Белевцева, В.Я. Настюк // Інформація і право, 2015. – № 2 (14). – С. 20-25.
2. Про інформацію: Закон України від 02.10.1992 № 2657-XII (із змінами) // Відом. Верхов. Ради України. – 1992 р. - № 48. – Ст. 650.
3. Конституція України від 28 червня 1996 р. // Відом. Верх. Ради України. – 1996. - № 30. – Ст. 141.

Солончук І.В.

старший викладач кафедри інформаційного права
та права інтелектуальної власності
Національного технічного університету України “Київський політехнічний інститут імені Ігоря Сікорського”

ІНФОРМАЦІЙНЕ СУДОЧИНСТВО: РЕАЛІЗАЦІЯ ПРАВА НА СУДОВИЙ ЗАХИСТ ПРАВ, СВОБОД ТА ІНТЕРЕСІВ ОСОБИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Сучасне суспільство є новітнім явищем, яке відображає еволюцію відносин у всіх сферах життєдіяльності людини. Як доводить значна кількість наукових досліджень останніх років, сьогодні суспільство є суспільством інформаційним, а отже, суспільством нового типу, де виникають, змінюються та припиняються інформаційні правовідносини [1, с. 29].

Інформаційне суспільство формує нову якість індивідуального й суспільного буття, яка полягає у тому, що кожна особистість забезпечується будь-якими знаннями. В свою чергу, це зумовлює радикальні зміни в системі суспільних відносин, як то політичних, правових, духовних та ін. [2, с. 9]. Вважаємо слушною думку деяких дослідників, які вбачають основну ідею інформаційного суспільства у соціогуманітарному вимірі як досягнення нової фази розвитку - “суспільства знань” та забезпечення для всіх рівного доступу до них [3]. Поняття інформаційного суспільства відображає об’єктивну тенденцію у соціальній еволюції, коли інформація (знання) стає однією з основних цінностей у житті людей [4]. Таким чином, розуміння прав та інтересів, свободи й відповідальності людини в сучасних умовах трансформується з урахуванням особливостей та властивостей інформаційних правовідносин.

Як вже зазначалося, інформаційні правовідносини є невід’ємним атрибутом життєдіяльності суспільства. В сучасному світі інформаційні правовідносини властиві всім, без винятку, сферам

соціального життя, які регулюються нормами права. На нашу думку, спостерігається надзвичайно стрімке поширення інформаційних правовідносин у сфери правового регулювання. Для прикладу пропонуємо звернути увагу на процесуальні правовідносини, які мають місце при здійсненні судами захисту прав, свобод та інтересів особи. Слід підкреслити, що судочинство в інформаційному суспільстві вже не може функціонувати в тому “класичному” розумінні, як це було ще кілька років тому. Сучасний розвиток суспільних відносин вимагає інформаційного судочинства, тобто судочинства нового типу, де мають місце інформаційні відносини, які належним чином регулюються, забезпечуються та захищаються у встановленому законом порядку [5, с. 249].

Конституція України в статті 55 проголошує право на захист прав та інтересів в судовому порядку [6]. Право на справедливий суд є засадою сучасного судочинства й гарантує кожному доступність правосуддя та захист прав, свобод, інтересів незалежним, безстороннім та справедливим судом, утвореним згідно вимог закону [7].

Відповідно до новел сучасної судової реформи в Україні у судах має функціонувати Єдина судова інформаційно-телекомунікаційна система (далі – ЄСІТС), власником якої є Державна судова адміністрація України (ДСА), а адміністратором і технічним розробником - державне підприємство “Інформаційні судові системи”. Точніше, за повідомленням ДСА України, ЄСІТС мала запрацювати з 2019 р. [8]. Зокрема, норми щодо діяльності ЄСІТС містить частина 1 ст. 14 Цивільного процесуального кодексу України (ЦПК), нова редакція якої набрала чинності з 15 грудня 2017 р. [9].

Структура ЄСІТС є складною та формується відповідно до Концепції побудови Єдиної судової інформаційної-телекомунікаційної системи, затвердженої Наказом Голови Державної судової адміністрації України від 13 квітня 2018 року №168[10]. Користувач має доступ до ЄСІТС через окремий “Електронний кабінет” (в Концепції ще використовується термін “офіційна електронна адреса”), що відкривається на сторінці офіційного веб-порталу судової влади України. Електронний кабінет надає змогу скористатись всіма актуальними сервісами ЄСІТС, наприклад, дізнатись інформацію щодо

місця, дати, часу розгляду судових справ та результату розгляду справ. Проаналізувавши положення Концепції, виникає запитання, чи доцільно ототожнювати категорії “Електронний кабінет” та “офіційна електронна адреса”? Не претендуючи на однозначність, спробуємо обґрунтувати власну позицію.

Складається ЄСІТС із декількох взаємопов’язаних підсистем: загальної; електронного діловодства; контакт-центру; управління фінансово-господарськими процесами; захисту інформації. Кожна підсистема, в свою чергу, включає окремі модулі. Наприклад, загальна підсистема включає шість модулів: 1) модуль “Офіційна електронна адреса (Електронний кабінет)”; 2) модуль “Офіційний веб-портал “Судова влада України”; 3) модуль “Єдиний державний реєстр судових рішень”; 4) модуль “Єдиний державний реєстр виконавчих документів”; 5) модуль “Відкриті набори даних”; 6) модуль “Автоматизована взаємодія з іншими автоматизованими системами”. А Єдина підсистема електронного діловодства судів, органів та установ системи правосуддя складається з п’яти модулів: 1) модуль “Електронний суд”; 2) модуль “Електронне діловодство”; 3) модуль “Автоматизований розподіл”; 4) модуль “Електронний архів; 5) модуль “Судова статистика”. Інші підсистеми також охоплюють окремі функціональні модулі. Отже, спостерігаємо нерозривну взаємодію судової реформи та використання новітніх інформаційних технологій. Як стверджує Т. Ткачук, масштабне впровадження інформаційних технологій і розвиток глобального інформаційного простору характеризує формування інформаційного суспільства [11, с. 61].

ЄСІТС має забезпечувати виконання широкого спектру завдань, зокрема, таких як: реєстрація в обов’язковому порядку заяв, скарг, інших передбачених законом процесуальних документів, які надходять до суду та можуть бути предметом судового розгляду; визначення судді або колегії суддів (судді-доповідача) для розгляду конкретної справи (автоматизований розподіл справ); забезпечення належного обміну документами (надсилання, отримання документів) в електронній формі між окремими судами, між судом та учасниками судового процесу, між учасниками судового процесу, фіксування судового процесу, забезпечення участі учасників су-

дового процесу у судовому засіданні в режимі відеоконференції; здійснення направлення судом судових рішень, судових повісток, інших процесуальних документів учасникам судового процесу на їхні офіційні електронні адреси та ін.

На жаль, сьогодні ЄСІТС в судах України функціонує лише в тестовому режимі, який передбачає роботу лише окремих її модулів, зокрема таких як: Єдиний контакт-центр судової влади України; Єдина підсистема управління фінансово-господарськими процесами; Офіційна електронна адреса (Електронний кабінет); Офіційний веб-портал “Судова влада України”; Єдиний державний реєстр судових рішень; Електронний суд; Автоматизований розподіл; Судова статистика. Як свідчать події останніх днів, використання досягнень технічного прогресу є необхідним для забезпечення нормального режиму роботи державних органів, в тому числі судів. У зв’язку з дією карантину, встановленого Кабінетом Міністрів України з метою запобігання поширенню коронавірусної хвороби (COVID-19), учасникам справи було дозволено брати участь у судовому засіданні в режимі відеоконференції поза межами приміщення суду з використанням власних технічних засобів. Для підтвердження особи учасника справи використовується електронний підпис, а якщо ж особа його не має, то підтвердження особи учасника справи відбувається у порядку, визначеному Законом України “Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус” або Державною судовою адміністрацією України [12]. Зрозуміло, що все це ефективніше б застосовувалося, якби робота ЄСІТС була налагодженою.

Основне питання, яке виникає на даному етапі – це належна ідентифікація особи, яка виступає учасником судочинства. Водночас, виникає ряд додаткових питань, зокрема щодо правового регулювання понять “офіційна електронна адреса” та “цифровий підпис”.

Сьогодні в наших правовідносинах не є обов’язковою наявність у особи офіційної електронної адреси. Більш того, даний термін потребує нормативного закріплення, оскільки ряд нормативно-правових актів (зокрема, ЦПК) ним оперують, а юридичне визна-

чення поняття відсутнє. Тому, на наш погляд, і виникають різні необґрунтовані тлумачення або ж ототожнення. Слід зазначити, що спроби юридично визначити поняття офіційної електронної адреси вже мали місце. Проект Закону “Про внесення змін до Закону України “Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань” щодо присвоєння офіційної електронної адреси під час державної реєстрації” від 22 грудня 2017 року містить пропозицію визначати офіційну електронну адресу як адресу електронної пошти юридичної особи, а також фізичної особи - підприємця, що використовується для офіційного листування в електронному вигляді, є незмінною до внесення запису про державну реєстрацію припинення юридичної особи, припинення підприємницької діяльності фізичної особи; листи та/або повідомлення, надіслані на офіційну електронну адресу, вважаються такими, що надіслані офіційно, та не потребують додаткового документального підтвердження” [13]. Даним проектом закону передбачалося присвоєння офіційних електронних адрес юридичним особам та ФОП одночасно з державною реєстрацією створення юридичної особи чи набуття статусу підприємця фізичною особою. Зазначені пропозиції не були враховані Верховною Радою України, оскільки 29 серпня 2019 р. даний проект закону був відкликаний.

Частиною 6 ст. 14 ЦПК України визначається обов’язок адвокатів, нотаріусів, приватних виконавців, арбітражних керуючих, судових експертів, державних органів, органів місцевого самоврядування, суб’єктів господарювання державного й комунального секторів економіки реєструвати офіційні електронні адреси в ЄСІТС. Для всіх інших осіб передбачається реєстрація офіційних електронних адрес в ЄСІТС в добровільному порядку. Реєстрація офіційної електронної адреси в ЄСІТС надає ряд переваг, оскільки після здійснення реєстрації всім цим особам суд надсилає будь-які документи у справах, в яких такі особи беруть участь, виключно в електронній формі шляхом їх направлення на офіційні електронні адреси цих осіб. Водночас, за особою зберігається право отримати копію судового рішення у паперовій формі, але для цього слід подати до суду окрему заяву. Також всі ці особи набувають можливості

подавати процесуальні, інші документи, вчиняти інші процесуальні дії в електронній формі за допомогою ЄСІТС, але за умови використання власного електронного цифрового підпису відповідно до Закону України “Про електронний цифровий підпис” [9]. Слід зазначити, що Закон України “Про електронний цифровий підпис” втратив чинність 7 листопада 2018р. (підстава 2155-VIII) [14].

В частині 1 ст. 1 Закону України “Про електронні довірчі послуги” визначаються поняття:

- *електронний підпис* – це електронні дані, які додаються підписувачем до інших електронних даних або логічно з ними пов’язуються і використовуються ним як підпис (пункт 12 частини 1);

- *кваліфікований електронний підпис* – це удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа (пункт 23 частини 1). Використання кваліфікованого електронного підпису забезпечує високий рівень довіри до схем електронної ідентифікації;

- *удосконалений електронний підпис* – це електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов’язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов’язаного з підписувачем, і який дає змогу здійснити електронну ідентифікацію підписувача, виявити порушення цілісності електронних даних, з якими пов’язаний цей електронний підпис (пункт 44 частини 1). Використання удосконаленого електронного підпису забезпечує середній рівень довіри до схем електронної ідентифікації [14].

Підсумовуючи викладене вище, хочемо зазначити, що на шляху до ефективного судочинства з використанням новітніх інформаційних технологій виникає багато перепон нормативного, організаційного та технічного характеру. На наш погляд, судочинство ще довго перебуватиме в стані постійного реформування, до поки держава не визначить, що забезпечення мережею інтернет є таким же необхідним для населення, як, наприклад, забезпечення електроенергією чи газопостачанням. Як слушно висловлюється О. А. Баранов, своєчасно вжиті юридичною науковою спільнотою зусилля

можуть дозволити отримати попереджувальні наукові результати і практичні рекомендації щодо правового регулювання суспільних відносин, що сприятиме широкому визнанню, швидкому впровадженню і поширенню прогресивних досягнень чергової технологічної революції [15, с. 70].

Список використаної літератури:

1. Солончук І. В. Інформаційні правовідносини: поняття та охорона. *Інформація і право*. № 4 (31)/2019. С. 28 – 36.
2. Дзьобань О.П., Рубан О. О. Свобода й відповідальність як аксіологічні маркери трансформації інформаційного суспільства. *Інформація і право*. 2020. № 1(32). Ст. 9-21.
3. Інформаційне суспільство в світі та Україні: проблеми становлення та закономірності розвитку: колективна монографія / за ред. д.ф.н., проф. В.Г. Воронкової. Запоріжжя: Вид-во ЗДІА, 2017. 292 с.
4. Дзьобань О. П., Кальницький Е. А. Зародження концептуальних підходів до розуміння сутності і специфіки інформаційного суспільства. *Вісник Національного університету «Юридична академія України імені Ярослава Мудрого»*. Серія: Філософія, філософія права, політологія, соціологія. 2013. Вип. 5 (19). С. 3-15.
5. Фурашев В. М., Солончук І. В. Інформаційне право: інформаційне судочинство. *Право та державне управління*. № 3 (36). Том 1. 2019. С. 241 – 251.
6. Конституція України: Закон України від 28 червня 1996 р. № 254к/96-ВР. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.
7. Про судоустрій і статус суддів: Закон України від 02 червня 2016 р. № 1402-VIII. *Відомості Верховної Ради*. 2016. № 31. Ст.545.
8. Структура Єдиної інформаційно-телекомунікаційної системи. Судова влада України: веб-сайт. URL: <https://dsa.court.gov.ua/dsa/inshe/esits/oiuty> (дата звернення: 22.02.2020).
9. Цивільний процесуальний кодекс України: Закон України від 18 березня 2004 р. № 1618-IV. *Відомості Верховної Ради України*. 2004. № 40-41, 42. Ст.492.
10. Наказ Голови Державної судової адміністрації України від 13 квітня 2018 року №168 “Про затвердження Концепції Єдиної судової інформаційно-телекомунікаційної системи”. URL: <https://dsa>.

court.gov.ua/dsa/inshe/esits/asdfg (дата звернення: 21.02.2020).

11. Ткачук Т. Сучасні домінанти інформаційного суспільства. *Інформаційна безпека: сучасний стан, проблеми та перспективи: матеріали I міжнародної науково-практичної конференції / КПП ім. Ігоря Сікорського*. Київ, 2019. 126 с.

12. Про внесення змін до деяких законодавчих актів України, спрямованих на забезпечення додаткових соціальних та економічних гарантій у зв'язку з поширенням коронавірусної хвороби (COVID-19): Закон України від 30 березня 2020 р. Голос України. № 62.

13. Про внесення змін до Закону України „Про державну реєстрацію юридичних осіб, фізичних осіб-підприємців та громадських формувань” щодо присвоєння офіційної електронної адреси під час державної реєстрації: Проект Закону від 22 грудня 2017 р. URL:http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=63226 (дата звернення: 21.02.2020).

14. Про електронні довірчі послуги:Закон України від 5 жовтня 2017 р. №2155-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 400.

15. Баранов О.А., Інтернет речей (IoT) і блокчейн. (ст. 59-71). *Інформація і право*. 2018. № 1(24). Ст. 59-71.

Ткачук Н.І.

кандидат юридичних наук
головний спеціаліст
Служба безпеки України

ОКРЕМІ ПИТАННЯ ЩОДО НАЦІОНАЛЬНИХ ТА МІЖНАРОДНИХ ЗАСАД ЗАХИСТУ ІНФОРМАЦІЙНИХ ПРАВ ТА СВОБОД ЛЮДИНИ

Сучасне українське суспільство є інформаційним, оскільки кількість, якості та ступінь використання інформації стають факторами, що визначають рівень розвитку держави й суттєво впливають на її статус у світовому співтоваристві. Становлення й розвиток інформаційних основ соціуму припускає наявність сукупності передумов, що забезпечують його відтворення й розвиток. Неодмінною умовою цього виступає правовий захист інформаційних прав та свобод людини й громадянина, які мають як юридичну, так і загально соціальну значущість та надають можливість забезпечувати взаємно необхідні відносини громадянина й держави.

Конституція відзначає, що кожний має право будь-якими, не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань [1]. Отже, засоби захисту прав та свобод людини і громадянина, в тому числі інформаційні, можуть бути класифіковані як судові, адміністративні і державні. Так, право громадян на судовий захист закріплене в ст.10 Загальної декларації прав людини [2] та у ст.55 Конституції України, відповідно до якої кожному гарантується право на оскарження в суді рішень, дій або бездіяльності органів державної влади, органів місцевого самоврядування, посадових і службових осіб [1]. При зверненні в суд людина може спиратися на положення Конституції України, норми якої є нормами прямої дії. Після використання всіх національних засобів юридичного захисту громадянин може звернутися за захистом своїх прав і свобод до відповідних міжнародних судових установ (Європейський суд з прав людини) або до відповідних органів міжнародних організацій (Комісія ООН з прав людини), членом або учасником яких є Україна. Адміністративна форма

захисту інформаційних прав та свобод людини і громадянина передбачає розгляд звернень громадян до вищих органів державної влади, органів місцевого самоврядування. Відповідно до ст. 40 Конституції України кожна людина має право направляти індивідуальне або письмове звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування, до посадових і службових осіб [1]. Особа може обирати будь-який засіб захисту своїх прав та свобод у випадку, якщо вона не задоволена результатами розгляду свого питання органами влади, підприємствами, установами та організаціями, посадовими особами тощо. Зазвичай адміністративна форма захисту передуює судовій. Щодо державного захисту прав та свобод людини і громадянина, в тому числі інформаційних, такий захист здійснюється через інститут Уповноваженого Верховної Ради з прав людини, про який йшлося вище.

Таким чином, правовий механізм захисту прав і свобод охоплює всі можливі дії щодо захисту інформаційних прав та свобод людини і громадянина, що відрізняє відповідну категорію від поняття «механізм реалізації людиною права на захист», яке, у свою чергу, позначає одну зі складових правового механізму захисту прав і свобод, сутність якої полягає у цілеспрямованій діяльності людини щодо відновлення становища, що існувало до порушення конкретного права особи [3, с. 34].

В сучасних умовах зміна пріоритетів Української держави на користь людини, її прав та свобод знаменує становлення демократичної концепції захисту прав та свобод людини і громадянина.

Реальне вдосконалення системи захисту інформаційних прав та свобод людини і громадянина в Україні є можливим за умови виявлення закономірностей функціонування, тенденцій розвитку, проблем правового механізму захисту інформаційних прав та свобод людини і громадянина, посилення його окремих складових та інституцій. Зокрема, слід враховувати, що правовий механізм захисту прав та свобод людини і громадянина містить організаційну та власне нормативно-правову складову, відтак за своєю суттю має організаційно-правовий характер.

Інформаційні права і свободи в Україні гарантуються Конституцією України та детально регламентується інформаційним за-

конодавством. Юридичні гарантії реалізації права на інформацію закріплюють відповідний обов'язок державних органів і їх посадових осіб сприяти громадянам у реалізації їх права на інформацію, а також інформувати про свою діяльність, прийняті рішення, створення в державних органах спеціальних інформаційних служб або систем, які б забезпечували у встановленому порядку доступ до інформації, застосування юридичної відповідальності за порушення законодавства про інформацію, здійснення державного контролю за його додержанням та інші.

Механізм юридичних гарантій реалізації інформаційних прав та свобод при цьому складається з наступних юридично значущих дій, що здійснюються уповноваженими державними органами: виконання юридичного обов'язку із забезпечення реалізації конституційного права на інформацію; створення необхідних умов для його реалізації; спостереження й контроль над реалізацією права; охорона інших інформаційних прав і свобод громадян, застосування санкцій у випадку їх порушення. Захист інформаційних прав та свобод може здійснюватися в неюрисдикційній формі (самозахист своїх прав і законних інтересів) і юрисдикційній формі (у спеціальному, адміністративному порядку або за загальним правилом у судовому порядку).

Стаття 34 Конституції визначає: «Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. Кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір. Здійснення цих прав може бути обмежене законом в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя». Згадане право є активним за своїм змістом, і становить можливість здійснювати будь-які дії щодо збирання, обробки, створення, зберігання та розповсюдження інформації у будь-якій формі, окрім випадків наявності прямих заборон з боку закону.

При цьому, з метою гарантування прав на доступ до інформації необхідно законодавче встановлення підстав для вирішення колізій при реалізації прав на інформацію й «права на таємницю», які б відповідали духу Глобальних принципів з національної безпеки і свободи інформації, котрі вказують, яка інформація, що перебуває у розпорядженні держави, може на законній підставі триматися в секреті, і яка інформація повинна бути розкрита [4]. У вітчизняному законодавстві також доцільно запровадити чіткий критерій обмеження інформаційних прав і свобод шляхом закріплення принципів такого обмеження, які виключають розширювальне або неоднозначне тлумачення.

Вирішенню низки актуальних проблем функціонування правового механізму захисту інформаційних прав та свобод людини і громадянина сприятиме оптимізація державної форми захисту прав і свобод шляхом введення посади «інформаційного омбудсмена» з використанням іноземного досвіду, а також запровадження чітких критеріїв обмеження інформаційних прав і свобод шляхом закріплення принципів такого обмеження, які виключають розширювальне або неоднозначне тлумачення.

Література:

1. Конституція України від 28 червня 1996 року. URL: zakon5.rada.gov.ua/laws/show/254k/96-вр
2. Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: http://zakon0.rada.gov.ua/laws/show/995_015
3. Сидорчук Ю.М. Механізми захисту прав людини та громадянина: сутність і перспективи розвитку в Україні. *Науковий вісник Чернівецького університету*. 2013, Випуск 682: Правознавство. С.33-35
4. The Global Principles on National Security and the Right to Information (The Tshwane Principles). URL: <https://www.opensocietyfoundations.org/publications/global-principles-national-security-and-freedom-information-tshwane-principles>

Забара І.М.

кандидат юридичних наук, доцент,
доцент кафедри міжнародного пра-
ва Інституту міжнародних відносин
Київського національного універси-
тету імені Тараса Шевченка

**АКТУАЛЬНІ ПИТАННЯ БЕЗПЕКИ І ЗАХИСТУ ПРАВ ЛЮДИНИ
В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИННИХ
ЗАХОДІВ: ОЦІНКИ, ПОЗИЦІЯ Й ІНІЦІАТИВИ ООН**

Значні і масштабні наслідки пандемії, а також її згубний вплив на добробут людей і держав, не залишилися поза увагою провідних міжнародних інституцій.

Організація Об'єднаних Націй зайняла центральну роль у справі активізації і координації глобальних заходів з недопущення і стримування поширення захворювання.

2 квітня 2020 року Генеральна Асамблея ООН прийняла Резолюцію №74/270 «Глобальна солідарність у боротьбі з коронавірусним захворюванням 2019 року (COVID-19)» [1]. В ній ООН наголосила про:

- загрозу здоров'ю, безпеці і добробуту людини, спричинену пандемією коронавірусного захворювання, яка продовжує поширюватись світом;

- безпрецедентні наслідки пандемії та її вплив,

- наслідки кризи в результаті пандемії, що можуть знівелювати успіхи, досягнуті в області розвитку та обмежити прогрес у досягненні цілей сталого розвитку людства;

- заходи, що пом'якшили б соціальні наслідки та увагу, яка необхідна для всеохоплюючого відновлення [1].

Було також акцентовано увагу на тих зусиллях, що уживають уряди держав, а також співробітники сфери охорони здоров'я та служб забезпечення у всьому світі у цілях боротьби із пандемією, захисту здоров'я і забезпеченню безпеки населення держав.

Так само було зазначено про необхідність усіх зацікавлених сторін спільно працювати на національному, регіональному і гло-

бальному рівнях визнаючи, що пандемія COVID-19 потребує прийняття заходів на основі єдності, солідарності й активного багатороннього співробітництва [1].

Разом з тим, на загальному фоні протидії у боротьбі з коронавірусним захворюванням (COVID-19) нагальною постала і задача в інформаційній сфері, зокрема, захист прав, свобод і безпеки людини в умовах карантинно-обмежувальних заходів.

Йдеться про протидію широкомасштабним світовим процесам поширення дезінформації про коронавірусне захворювання (COVID-19) та наслідкам її поширення. Генеральний секретар ООН А. Гутерріш, у своєму спеціальному відео-зверненні наголосив на тому, що *«Світ сьогодні об'єднався у боротьбі з пандемією COVID-19, що призвела до кризи, якої він не знав з часів Другої світової війни. Але сьогодні ми стаємо свідками ще однієї небезпечної епідемії – епідемії дезінформації»*[2].

Ситуація, яка склалася, характеризується тим, що у зв'язку з карантинно-обмежувальними заходами, більшість переносить свою діяльність у сферу інформаційно-комунікаційних технологій. Наслідком є збільшення світового інформаційного трафіку у три (!) рази. Це має як позитивні, так і негативні наслідки.

У цій ситуації поширення неперевіреної інформації, а у переважній більшості – цілеспрямованої і масштабної дезінформації про коронавірусне захворювання (COVID-19) у медійному просторі і соціальних мережах супроводжується наступним:

- наявністю широкої аудиторії, яка значну частину часу перебуває онлайн, де, серед іншого, відбувається пошук незадоволених і зневірених, як потенційних жертв інформаційних маніпуляцій;

- масштабністю поширення (зазначимо, що за даними ООН, боти генерують до 40% дезінформаційних повідомлень про коронавірусне захворювання;

- навмисним поширенням дезінформації, зокрема заяв, тверджень і звинувачень антикитайського, антиісламського, антисемітського спрямування (як приклад, про «теорії змови»);

- закликами до «пошуку крайніх» (осіб або держав);

Особами, проти яких спрямовується неправдива і перекручена інформація, за цих умов, як правило, виступають:

- іноземці, мігранти, біженці (іноді і власні громадяни, що повертається на батьківщину), яких розглядають в якості джерела небезпеки;
- люди літнього віку (які є найбільш вразливими);
- особи, що професійно виконують свої обов'язки і доносять правдиву інформацію про справжній стан перебігу подій (журналісти, працівники сфери охорони здоров'я і служб, що надають допомогу, а також правозахисники).
- керівні органи держав, окремі організації (за партійною та іншою приналежністю).

Як наслідок, поширення дезінформації про коронавірусне захворювання (COVID-19) супроводжується:

- нагнітанням страху, безвиході, песимістичними прогнозами;
- проявами агресії і ненависті до:
- іноземців, мігрантів і біженців, що розглядаються в якості джерела поширення вірусу, з наступними закликами позбавити їх медичної допомоги;
- людей похилого віку, що має появ через образливі заклики і зображення, що прирівнюють їх до статусу малоцінних;
- арештом журналістів (майже 250 журналістів перебувають під арештом).

Усе наведене утворюється в інформаційній сфері таким феноменом, який отримав назву «мова ненависті». Для потенційних жертв саме з його допомогою утворюється атмосфера безвиході, зневіри, апатії, песимізму.

Разом з тим, у відповідь на протидію широкомасштабним світовим процесам поширення дезінформації про коронавірусне захворювання (COVID-19) та наслідкам її поширення, ООН розпочала процес протидії, розгорнувши нову програму – *«Ініціативу боротьби з дезінформацією про COVID-19»*. Ініціатива ґрунтується на науковому підході до проблеми, а також заклику до об'єднання у пошуку рішень для боротьби з дезінформацією[3].

За даними офіційних осіб ООН, діяльність в рамках цієї Ініціативи відбувається за кількома напрямками [3], а саме:

1. Збирання фактів та поширення достовірних відомостей

За цим напрямком Всесвітня Організація Охорони Здоров'я (ВООЗ) надає і поширює перевірену інформацію, засновану на наукових даних.

ВООЗ, з метою поширення правдивої, науково достовірної та перевіреної інформації, утворила *Мережу з епідемічних захворювань*. До мережі приєднані групи технічних і соціальних ЗМІ. Ці групи відслідковують і спростовують дезінформацію, міфи, чутки, а також надають достовірні відомості і докази для прийняття адекватних заходів. До цього процесу долучені 59 інформаційних центрів ООН за кордоном, які у свою чергу сприяють боротьбі з недостовірною інформацією місцевими мовами [3].

2. Співробітництво з великими компаніями

ВООЗ, у співробітництві з компаніями WhatsApp і Facebook запустила програму інформаційних розсилок арабською, англійською, французькою, гінді, італійською, португальською та іспанською мовами саме для поширення рекомендацій, у зв'язку з пандемією COVID-19. Охоплена такою інформацією аудиторія складає 2 мільярди осіб. Розсилки безпосередньо надходять від ВООЗ.

У рамках співробітництва ВООЗ і Rakuten Viber було утворено інтерактивний чат-бот, що надає інформацію про COVID-19. В такий спосіб більше 1 мільярда осіб отримує інформацію рідними мовами за допомогою мобільних телефонів.

ВООЗ і Міжнародний союз електрозв'язку (МСЕ), за підтримки Дитячого фонду ООН (ЮНІСЕФ) закликали телекомунікаційні компанії в усіх державах світу приєднатися до Ініціативи, яка дозволить зберегти життя в період пандемії COVID-19 за допомогою текстових повідомлень. Цей напрям спрямований на аудиторію у 3,6 мільярда осіб по всьому світу, що не має виходу до Інтернету [3].

3. Взаємодія з журналістами і ЗМІ

Організація Об'єднаних націй з питань освіти, науки і культури (ЮНЕСКО) опублікувала дві аналітичні записки, у яких надана оцінка «епідемії дезінформації» у період пандемії. Записки також містять інформацію Міжнародного центру для журналістів який, у свою чергу, також допомагає професійним журналістам, які працюють у різних країнах світу безпосередньо в період «епідемії дезінформації» забезпечувати населення надійними, точними і достовірними даними з питань суспільного здоров'я.

4. Робота з громадянським суспільством

ООН співпрацює з численними організаціями громадянського суспільства, які мають асоційований статус при Департаменті глобальних комунікацій ООН і Економічній і Соціальній Раді ООН (ЕКОСОП).

Департамент глобальних комунікацій ООН надає ключову інформацію для неурядових організацій щодо їх участі у процесах і заходах високого рівня на майданчиках ООН. Щотижневий інформаційний бюлетень охоплює 1900 організацій по всьому світу, поширюючи інформацію і, одночасно, отримуючи дані про неправдиві відомості, стереотипи і міфи, що поширюються світом і перешкоджають проведенню відповідних заходів на глобальному рівні [3].

5. Правозахисна діяльність

Діяльність у цьому напрямку спрямована проти обмежувальних заходів, введених низкою держав проти незалежних ЗМІ та журналістів.

Підсумовуючи, зауважимо, що діяльність ООН і інших міжнародних організацій, враховуючи значні і масштабні наслідки пандемії, продовжується і буде доповнюватись новими програмами боротьби з «епідемією дезінформації».

Перелік джерел

1. Резолюція №74/270 «Глобальна солідарність у боротьбі з коронавірусним захворюванням 2019 року (COVID-19) URL: [OON_Rezol_COVID-19.pdf](#)

2. Глава ООН: мы должны противопоставить лжи оCOVID-19 факты и научные данныеURL:[http:news.un.org/ru/story/2020/041376212](#)

3. ООН предлагает пять способов для борьбы с «эпидемией» дезинформации о COVID-19 URL:[http:news.un.org/ru/coronavirus/five-ways-united-nations-fightinginfodemic-misinformationn](#)

Юник І. Г.

кандидат наук з державного управління,
доцент,
доцент кафедри правових наук та
філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського

РЕАЛІЗАЦІЯ ПРАВА НА ДОСТУП ДО ПУБЛІЧНОЇ ІНФОРМАЦІЇ ЯК МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ПРОЗОРОСТІ ТА ВІДКРИТОСТІ ВЛАДНИХ ІНСТИТУЦІЙ

Забезпечення доступу до публічної інформації є одним із важливих показників відкритості та прозорості владних інституцій. Об'єктивними показниками ефективності забезпечення прозорості та відкритості владних інституцій є позиція держави у відповідних міжнародних рейтингах. Так, у 2018 р., згідно з показниками Індексу глобальної конкурентоспроможності Україна з-поміж 140 держав займає 110-е місце – за рівнем розвитку державних інститутів, 77-е місце – за рівнем адаптації технологій, 58-е – за рівнем інноваційних можливостей.

Основними законодавчими документами, що регулюють реалізацію права на доступ до публічної інформації є закони України “Про інформацію”, “Про доступ до публічної інформації”, “Про державну службу”.

Порядок здійснення та забезпечення права кожної людини на доступ до інформації в Україні забезпечує Закон України “Про доступ до публічної інформації”. Відповідно до цього закону, публічною інформацією є відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень[1].

На сьогодні доступ до публічної інформації забезпечується шляхом систематичного та оперативного оприлюднення в офіційних

друкованих виданнях, на офіційних веб-сайтах в мережі Інтернет, єдиному державному веб-порталі відкритих даних, інформаційних стендах, а також може надаватися інформація за запитами на інформацію тощо.

За порядком доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом – конфіденційну інформацію, таємну інформацію, службову інформацію. Доступ до публічної інформації здійснюється на принципах прозорості та відкритості діяльності владних інституцій, вільного отримання, поширення та будь-якого іншого використання інформації, а також рівноправності.

Варто зауважити, що сьогодні владні інституції України досить багато уваги надають питанню оприлюднення інформації. Так, для реалізації права на доступ до публічної інформації Офіс Президента України керується низкою нормативно-правових актів, які регулюють:

- забезпечення доступу до публічної інформації в допоміжних органах, створених Президентом України (2019 р.);
- організацію роботи щодо забезпечення в Офісі Президента України доступу до публічної інформації (2019 р.);
- перелік відомостей, що становлять службову інформацію в Адміністрації Президента України» (2017 р.);
- систему обліку публічної інформації в Адміністрації Президента України (2016 р.) тощо.

З метою забезпечення безумовного виконання Закону України “Про доступ до публічної інформації” Кабінет Міністрів України, центральні органи виконавчої влади, місцеві державні адміністрації розробили і затвердили власні форми та порядок подання запиту на інформацію, запровадили облік запитів на інформацію, визначили спеціальні структурні підрозділи та посадових осіб, які організовують доступ до публічної інформації, а також забезпечують оприлюднення публічної інформації в офіційних друкованих виданнях, на веб-сайтах, інформаційних стендах та інші способи, прийнятні для громадян.

За результатами аналізу інформації, отриманої Управлінням забезпечення доступу до публічної інформації Департаменту інфор-

мації та взаємодії з громадськістю Секретаріату Кабінету Міністрів у 2019 р. органи виконавчої влади отримали та опрацювали 95 478 запитів на інформацію, серед яких 25 % від загальної кількості запитів надійшло до міністерств, 57,4 % – до інших центральних органів виконавчої влади та 17,6 % – до місцевих органів виконавчої влади. Найбільше запитів надійшло до Національної поліції (26006), Міністерства внутрішніх справ (7153), Пенсійного фонду (6956), Київської міської держадміністрації (5776), Міністерства юстиції (2918), Державної фіскальної служби (2395), Адміністрації Держприкордонслужби (2374), Міністерства охорони здоров'я (2120), Міністерства соціальної політики (2017) тощо. Переважну більшість запитувачів у 2019 р. цікавила інформація про товар (роботу, послугу) (18663 запити), правова інформація (13000 запитів), інформація про фізичну особу (12498 запитів), статистична інформація (8970 запитів) та інформація довідково-енциклопедичного характеру (6477 запитів) [2].

У контексті реалізації права на доступ до публічної інформації, Кабінет Міністрів України звітує про надходження запитів та запровадив систему обліку публічної інформації. Також Кабінет Міністрів України організував роботу щодо запитів на інформацію у Секретаріаті Кабінету Міністрів. Так, у 2019 р. до Секретаріату Кабінету Міністрів України надійшло 3812 запитів. Здебільшого запитувачів цікавить інформація довідково-енциклопедичного змісту (44 %), правова інформація (22 %) та інформація про фізичну особу (11 %). У регіональному розрізі найбільше запитів надійшло з м. Києва, Одеської, Львівської, Харківської, Дніпропетровської, Київської та Донецької областей.

На підставі Закону України “Про доступ до публічної інформації” місцеві державні адміністрації також розробили порядок доступу до публічної інформації з метою реалізації права кожної людини на доступ до публічної інформації. Цей порядок регламентує питання обов'язкового оприлюднення публічної інформації, приймання, реєстрації та розгляду запитів фізичних, юридичних осіб, об'єднань громадян без статусу юридичної особи, надання інформації, відтермінування та відмови у її наданні, розгляду скарг на рішення, дії чи бездіяльність розпорядників інформації.

Для реалізації права на доступ до публічної інформації, місцеві державні адміністрації визначили та затвердили:

- перелік видів публічної інформації, розпорядником якої вони є;
- перелік відомостей, що становлять службову інформацію, і яким надається гриф “Для службового користування”;
- порядок оприлюднення актів місцевих державних адміністрацій;

положення про функціонування офіційного веб-порталу відповідної місцевої державної адміністрації.

У 2016 р. за результатами дослідження Центру демократії та верховенства права у рамках проекту Платформа “Омбудсман Плюс” найкращі показники щодо дотримання та виконання законодавства про доступ до публічної інформації серед обласних державних адміністрацій мають Вінницька, Сумська і Дніпропетровська обласні державні адміністрації, а найгірший рейтинг у Київської, Харківської та Донецької облдержадміністрацій.

Також важливу роль у контексті доступу до публічної інформації має Закон України “Про державну службу”, який зобов’язує керівників органів виконавчої влади щорічно опубліковувати та виступати з публічним звітом про підсумки діяльності відповідного державного органу за участю представників громадських рад, громадських об’єднань, організацій роботодавців, професійних спілок, некомерційних організацій, експертів відповідних галузей та засобів масової інформації. У публічному звіті має бути інформація про результати роботи органу виконавчої влади та аналіз діяльності органу виконавчої влади, інформація про використання коштів державного бюджету, організаційна інформація, а також інша інформація в межах компетенції органу виконавчої влади, що може бути винесена на публічне обговорення.

На сьогодні поступово відбувається модернізація діяльності владних інституцій у контексті реалізації права на доступ до публічної інформації через затверджені “Стратегію реформування державного управління України на 2016-2020 роки” та “Концепцію розвитку електронного урядування в Україні”. Відповідно до зазначених нормативно-правових актів, владні інституції мають забезпечити розвиток відкритих даних, зокрема:

- сформувати та запустити функціонування Єдиного державного веб-порталу відкритих даних, інтегрованих з ним інших веб-порталів відкритих даних;

- оприлюднення пріоритетних наборів даних у формі відкритих даних відповідно до суспільного інтересу на національному та регіональному рівні;

- проведення моніторингу стану оприлюднення та оновлення наборів даних на офіційних веб-сайтах державних органів та на Єдиному державному веб-порталі відкритих даних.

Оприлюднення публічної інформації у формі відкритих даних для вільного використання дасть змогу створити ефективний механізм реалізації права людини на доступ до публічної інформації та загалом підвищити прозорість і відкритість діяльності владних інституцій.

Однак, попри наявні деякі успіхи, ще є досить багато проблемних моментів реалізації права громадян на доступ до публічної інформації, серед яких:

- безпідставна відмова органами влади у наданні публічної інформації, відносячи її до інформації з обмеженим доступом;

- часто неправомірно застосовують грифи обмеження доступу до інформації;

- органи влади не повністю виконують вимогу оприлюднювати інформацію про свою діяльність тощо.

Список використаної літератури

1. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-1> (дата звернення: 17.05.2020).

2. Робота із запитами на інформацію у 2019 році// Кабінет Міністрів України: веб-сайт.URL: <https://www.kmu.gov.ua/gromadskosti/dostup-do-publichnoyi-informaciyi/rezultati-anketuvannya-organiv-vikonavchoyi-vladi-ta-monitoringu-oficijnih-veb-sajtiv/robo-ta-iz-zapitami-na-informaciyu-u-2019-roci>.

Ірха Ю.Б.,

кандидат юридичних наук, заслужений юрист України,
старший науковий співробітник
Державного науково-дослідного
інституту МВС України

ПРАВОВА ПОІНФОРМОВАНІСТЬ НАСЕЛЕННЯ УКРАЇНИ ЯК ОДНА З ГАРАНТІЙ ДОСТУПУ ГРОМАДЯН ДО ПРАВОСУДДЯ

У ХХІ ст. важко уявити повсякденне життя людини без Інтернету, комп'ютерів, мобільних телефонів та інших досягнень науки і техніки. Сучасні технології суттєво покращили можливості створення, зберігання, одержання та обміну інформацією. Високотехнологічні пристрої використовуються не тільки на професійному, але й на побутовому рівні, що полегшує задоволення різноманітних потреб індивідів. У багатьох випадках маленькі діти краще за батьків, а особливо бабусь і дідусів, вміють користуватися смартфонами, планшетами, ноутбуками, Smart-TV тощо. Технологічна обізнаність є загально визнаною вимогою часу, без якої людині досить важко розвиватися в інформаційному суспільстві.

Поряд зі стійким розумінням необхідності опанування нових технологій, у значної кількості людей досі існують серйозні прогалини у знаннях щодо належних їм прав і свобод, а також національних і міжнародних механізмів їх охорони і захисту. В умовах вільного доступу до правової інформації, публічності органів державної влади та органів місцевого самоврядування, безперешкодної участі громадськості у суспільно-політичному та соціально-економічному дискурсі, в Україні продовжують існувати труднощі у забезпеченні громадянам доступу до правосуддя. Однією з причин цього є низький рівень правової поінформованості населення, передусім вразливих та незахищених верств, внаслідок чого вони: не знають про наявність у них відповідних прав і свобод, можливостей та способів їх реалізації; невчасно звертаються за правовою допомогою, а також до суду, правоохоронних органів та інших

уповноважених суб'єктів за охороною і захистом своїх прав і свобод; не можуть швидко поновити свої права і свободи, отримати відшкодування завданої шкоди; є вразливими до маніпуляції їх поведінкою, зловживання довірою, втрати рухомого чи нерухомого майна.

Ще у 1993 році В. Боєр наголошував на важливості забезпечення правової поінформованості населення. На його переконання, правова поінформованість є критерієм, який визначає ступінь оволодіння правовою інформацією, з огляду на освіту людини, її правовий досвід, соціальний статус, інтереси та психологічні установки. Правова поінформованість є дієвим інструментом реалізації творчої ролі права та дозволяє громадянам найбільш повно використовувати їхні демократичні права і свободи. Вона сприяє формуванню поваги до правового закону, розвиває правове мислення, формує правову культуру, стимулює соціально зрілу поведінку особи у правовій сфері [1].

За твердженнями Д. Александрова правова поінформованість – це знання групою та її членами законів та інших правових настанов, як уже діючих, так і нових, що розробляються суб'єктами правотворчості, а також уміння орієнтуватися в них при прийнятті рішень, котрі стосуються власного життя і діяльності. Цей компонент не може бути сформований раз і назавжди. Він може знаходитися на належному рівні розвитку, якщо: потрібна людям інформація постійно до них надходить; це відбувається відповідно до вимог часу і потреб громадян; надходження такої інформації та коментарі до неї надаються компетентними людьми та характеризуються вірогідністю [2].

Правова поінформованість людини, як зазначає Р. Осіпов, є найголовнішим фактором її законослухняності та правомірної активності. Суспільний розвиток можливий тільки у разі підтримки на належному рівні дисципліни і правопорядку, що досягається знанням, розумінням і прийняттям громадянами офіційно закріплених правил поведінки в державі. Правова поінформованість важлива як для особи, так і для держави. Високий та якісний рівень поінформованості сприяє не тільки повній реалізації прав, свобод та законних інтересів людини, але й розвитку демократії, підвищення

ефективності управління, зміцненню законності і правопорядку в держави. Це своєрідний «місток» між змістом юридичних приписів та їх втіленням у життя [3, с. 305, 308].

На переконання Н. Бровко для того, щоб володіти певним багажем правових знань, формувати правові погляди, уявлення, почуття, настрої, оцінки правових явищ, необхідно для початку отримати правову інформацію. Недостатня інформація здійснює такий же негативний вплив на правосвідомість, як і надмірна. Отримавши ту чи іншу інформацію правового змісту, особа інтерпретує її відповідно до власних соціальних установок, позицій, поглядів, переконань. Кожен суб'єктивно підходить до вибору правової норми в конкретній ситуації й використовує лише ту, яка, на його думку, його стосується. Тому та кількість правової інформації, яка для однієї людини буде вважатися достатньою, для іншої буде недостатньою. Вищим показником правової інформованості є наявність навичок і вмінь користуватися отриманою правовою інформацією, правильно інтерпретувати й усвідомлено доносити її [4, с. 148].

Високий рівень правової поінформованості суспільства, як зауважує Я. Дупай, створює для всіх його членів можливість користуватися юридичними приписами на основі їх знання, а це в свою чергу знаходить свій вираз у здатності керуватися ними у своїй поведінці і безпосередній діяльності. Умови, які визначають рівень правової поінформованості суспільства, безпосередньо пов'язані з удосконаленням діяльності держави на шляху побудови сучасного інформаційного простору, підвищення ефективності функціонування системи державних органів, що створюють законодавство, підтримують його в дієвому стані, а також інформують про зміст його приписів [5, с. 54].

Генеральна Асамблея ООН у декларації наради на високому рівні «Верховенство права на національному і міжнародному рівнях», вказала на необхідності забезпечення для всіх людей рівного доступу до системи правосуддя та важливості підвищення інформованості населення про юридичні права (пункт 14). У Рекомендації R (81) 7 стосовно шляхів полегшення доступу до правосуддя Комітет міністрів Ради Європи запропонував державам-членам вживати необхідних заходів для інформування громадськості про

засоби захисту прав кожної особи в судовому порядку. Державам рекомендовано здійснювати інформування про місцезнаходження і компетенцію судів; порядок звернення до суду та захисту своїх інтересів у судовому порядку. Наголошено, щоб в судах або в інших компетентних органах була оприлюднена інформація щодо процесуальних норм, за умови відсутності юридичних порад по суті справи; порядку звернення до суду і строки, впродовж яких можливий розгляд такого звернення; процесуальні вимоги та необхідні для цього документи; засоби виконання судового рішення та можливі супутні витрати (пункти 1, 2).

Консультативна рада європейських суддів у Висновку № 6 (2004) зазначила, що доступ громадян до правосуддя передбачає надання належної інформації про функціонування судової системи. Громадськість має усвідомлювати природу судового провадження, його можливу тривалість, вартість та ризики неправильного використання юридичної системи. Крім того, варто забезпечити надання інформації про альтернативні засоби врегулювання спорів, які можуть бути запропоновані сторонам. Ця інформація може доповнюватися відомостями щодо важливих судових рішень (пункти 11–14).

У Висновку № 7 (2005) Консультативна рада європейських суддів наголосила, що громадяни повинні отримувати належну інформацію про організацію органів публічної влади та умов, в яких створюються закони. Для громадян важливо знати про те, як функціонують установи судової системи. Правосуддя є важливим компонентом демократичних суспільств, його метою є вирішення спорів між сторонами і, шляхом прийняття рішень, виконання як «нормативної», так і «просвітницької» ролі, надаючи громадянам відповідні настанови, інформацію та запевнення щодо права і його практичного застосування. Адекватна інформація про функції судової влади та її роль у повній незалежності від інших гілок державної влади може сприяти більшому розумінню функціонуванню судів, а також обмежень в їхній діяльності (пункти 6, 7, 8).

Фахівцями Програми розвитку ООН виокремлено фактори, які послаблюють систему правосуддя, зокрема, низький рівень грамотності населення, відсутність належної інформації про законодавче регулювання і судову практику, обмеженість загально-

відомих знань про права; відсутність належних систем правової допомоги; надмірна кількість законів [6, с. 4]. На переконання європейської дослідниці В. Терцієвої право на доступ до правосуддя гарантує кожній людині доступ до незалежного і неупередженого суду, справедливий і законний судовий розгляд у випадках, коли існує загроза свободі або майну особи. Це право тісно пов'язане із правовою грамотністю населення [7, с. 214].

Американський професор Т. Марчіорі вважає, що здатність громадян звертатися до органів правосуддя з метою задоволення їх скарг та вирішення конфліктів є суттєвим елементом верховенства права, демократії, прав людини та розвитку загалом. Науковець наголошує, що доступ до правосуддя вимагає наявності в державі: належної законодавчої бази, яка забезпечує всебічні та рівні права усім громадянам відповідно до міжнародних стандартів у сфері захисту прав людини; доступних та посильних юридичних консультацій та представництва інтересів; ефективних та неупереджених механізмів виконання судових рішень; доступних, посильних, своєчасних, ефективних, кваліфікованих, неупереджених, некорупційних механізмів вирішення спорів, яким довірять громадяни; висока правосвідомість та правова грамотність населення [8, с. 11].

Згідно з Конституцією України людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю; 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; в Україні визнається і діє принцип верховенства права; кожному гарантується знати свої права і обов'язки (стаття 3, частина перша статті 8, частина перша статті 57).

Зазначені конституційні положення зобов'язують державу здійснювати заходи щодо побудови і розвитку демократичного суспільства, зокрема шляхом інформування населення про напрями здійснення внутрішньої і зовнішньої політики; існуюче правове регулювання та перспективи його зміни і вдосконалення; особливості функціонування органів публічної влади та порядок звернення до них. При цьому важливо, щоб особа не тільки володіла певною

правовою інформацією, але й вміла застосовувати її на практиці, адже як слушно звертає увагу У. Настояща, людина може мати тільки загальні уявлення про правову систему в суспільстві і зовсім не знати детальну сутність законів та механізмів їх у роботі [9, с. 192]. Уважається, що з метою забезпечення законності та правопорядку в нашій державі мають бути створені ефективні механізми не тільки поширення інформації про існуючі права, свободи і обов'язки, але й можливості та способи їх реалізації, охорони і захисту, насамперед в органах правосуддя.

В Україні з кожним роком розвиваються механізми поширення правової інформації серед населення. У 2006 році в Концепції вдосконалення судівництва для утвердження справедливого суду в Україні відповідно до європейських стандартів, затвердженої Президентом України, було визначено, що «однією з важливих умов доступності правосуддя є поінформованість особи про організацію і порядок діяльності судів; правосуддя не стане доступним, якщо система судів лишатиметься для особи складною та незрозумілою щодо визначення компетентного суду для вирішення її справи». Згідно з цією концепцією передбачалося, що подальший розвиток правосуддя в Україні «має бути спрямований на утвердження верховенства права через забезпечення: доступності правосуддя; справедливої судової процедури; незалежності, безсторонності та професіоналізму суддів; юридичної визначеності, однаковості судової практики і відкритості судових рішень; ефективності судового захисту».

У Стратегії інформування громадян про гарантовані їм Конституцією та законами України права на період до 2019 року, затвердженої Кабінетом Міністрів України, наголошено, що «кризовий стан в умовах тимчасової окупації частини території України та військової агресії Російської Федерації та його прояви призводять до стійкого соціального та правового нігілізму, а нігілістичні настрої – до несприйняття права як найдієвішого регулятора суспільних відносин і, як наслідок, заважають формуванню відповідного сучасним реаліям правового світогляду. Це зумовлює певну не завжди бажану для суспільства поведінку особи. З огляду на зазначене необхідним є відродження поваги до закону, принципів вер-

ховенства права та законності, підвищення авторитету закону, що є першочерговим завданням для представників вітчизняної наукової, юридичної, політичної еліти, а також громадянського суспільства в цілому».

На виконання цієї стратегії Міністерством юстиції України упродовж 2017–2019 рр. був реалізований загальнонаціональний правопросвітницький проект «ЯМАЮ ПРАВО!». Водночас на початку 2020 року Уряд України без обґрунтування не продовжив дію зазначеної стратегії та проекту, а також не повідомив про майбутні плани з реалізації конституційного обов'язку держави щодо правового просвітництва населення.

Опрацювання питань підвищення рівня правової поінформованості громадян дає підстави стверджувати, що в Україні найбільші труднощі у доступі до правосуддя мають малозабезпечені та соціально вразливі верстви населення, а також внутрішньо переміщені особи, люди, які проживають у сільській місцевості, на окупованих територіях та в зоні проведення операції Об'єднаних сил. Саме через необізнаність цих людей про наявні правозахисні механізми (у тому числі безкоштовні) вони не звертаються або звертаються із запізненням до органів правосуддя (суд, адвокатура, прокуратура) чи інших інституцій.

З метою захисту прав і свобод людини і громадянина, недопущення виникнення соціальної напруженості, забезпечення законності та правопорядку вважається за доцільне на місцевому рівні розвивати механізми правового інформування та виховання громадян через можливості системи безоплатної правової допомоги, територіальних органів юстиції, юридичних клінік закладів вищої освіти, юридичних підрозділи місцевих органів публічної влади, громадських організацій.

Перелік використаних джерел

1. Боєр В. М. Правовая информированность и формирование правовой культуры личности (вопросы теории) : автореф. дис. ... канд. юрид. наук : 12.00.01. Санкт-Петербург., 1993. 22 с. URL: <http://www.law.edu.ru/article/article.asp?articleID=1171780> (дата звернення 15.05.2020).

2. Александров Д.О. Юридична психологія: підручник / за заг. ред. Л.І.Казміренко, Є.М.Моїсєєва. Київ : КНТ, 2007. 360с. URL: https://pidruchniki.com/13560615/psihologiya/pravova_ideologiya (дата звернення 15.05.2020).

3. Осипов Р.А. Правовая информированность: понятие и структура. Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. №1 (33). С. 305–309.

4. Бровко Н.І. Правова інформованість та її вплив на правосвідомість жителів сільської місцевості. Науковий вісник Херсонського державного університету. 2017. Вип. 6. Т. 3. С. 146–149.

5. Дупай Я.М. Правова інформованість суспільства як необхідна умова функціонування правової системи Часопис Київського університету права. 2015. № 4. С. 53–56.

6. AccesstoJustice. Practice Note. UNDP. 2004. 31 p. URL:https://www.undp.org/content/dam/aplaws/publication/en/publications/democratic-governance/dg-publications-for-website/access-to-justice-practice-note/Justice_PN_En.pdf(дата звернення 15.05.2020).

7. Edwin Rekosh, Kyra A. Buchko, Vessela Terzieva. Pursuing the Public Interest: A Handbook for Legal Professionals and Activists, New York, 2001. 355 p.URL: <https://www.pilnet.org/public-interest-law-resources/35-pursuing-the-public-interest-a-handbook-for-legal.html> (дата звернення 15.05.2020).

8. Teresa Marchiori. A Framework for Measuring Access to JusticeIncluding Specific Challenges Facing Women. UN Women. Council of Europe. 2015. 147p. URL: <https://rm.coe.int/1680593e83https://rm.coe.int/1680593e83> (дата звернення 15.05.2020).

9.Настояща У.В. Психологічні аспекти правової свідомості як детермінанти особистості співробітника Державної кримінально-виконавчої служби України. Кримінально-виконавча система: Вчора. Сьогодні. Завтра. 2018. № 1 (3). С. 182–197.

Богущий П.П.

кандидат юридичних наук, доцент,
головний науковий співробітник
Науково-дослідного інституту ін-
форматики і права НАПрН України

ІНФОРМАЦІЙНА ПРИВАТНІСТЬ І ПУБЛІЧНІСТЬ ЯК СУТНІСНІ ОЗНАКИ ІНФОРМАЦІЙНО-ПРАВОВИХ КОМУНІКАЦІЙ

Інформаційну сферу сучасного суспільства утворюють багаточисленні інформаційні комунікації, множинність яких лише умовно можна вважати системною. Інформаційні комунікації виникають, існують, зазнають трансформації і припиняють своє існування в інформаційному просторі як окремі мікросистеми, що мають здатність об'єднуватися у системи вищого порядку на основі визначених учасниками комунікацій об'єкта та мети. Водночас учасники інформаційних комунікацій в усіх випадках мають певні ознаки суб'єктності, адже вступають у комунікації як носії певних правомочностей та правозобов'язань, або ж – як суб'єкти узгодження власної поведінки стосовно значущої для кожного інформації.

За таких обставин, зважаючи на правові ознаки учасників інформаційних комунікацій, справедливим є висновок про те, що інформаційні комунікації завжди є інформаційно-правовими комунікаціями або ж інформаційними правовідносинами [1, с.21-23], що визначає їхню сутнісну характеристику. Дійсно, сьогодні неможливо уявити процес утворення, збирання, зберігання, передачі інформації без упорядкування діяльності певними нормами права. Тут можна не обмежувати дискурс виключно офіційним правом або ж законодавчим правом, розуміючи під законодавством будь-які норми, що мають державне, владне походження. Річ у тому, що інформаційні комунікації зазнають впливу локального нормотворення, яке є доречним з огляду на специфіку окремих комунікативних систем. З іншого боку особливості сучасного суспільства, як мережевого суспільства, виявляються в існуванні певних соці-

ально значущих утворень, які продукують свої інтереси, формалізують інтереси до рівня обов'язкових правил і зосереджуються над забезпеченням їхньої реалізації. У таких мережових соціально значущих утвореннях інформаційна діяльність має свою специфіку, засновану на внутрішньомережових вимогах, які часто не співпадають із загальносуспільними, а суперечності, що виникають, потребують відповідного реагування та вирішення інформаційним правом або ж правом інформаційної безпеки в залежності від гостроти та актуальності суперечностей і можливих конфліктів.

Суб'єктність учасників інформаційно-правових комунікацій визначається публічно-правовою природою діяльності щодо утворення, збирання, зберігання, передачі інформації, обміну інформацією. Проте в інформаційно-правових комунікаціях надважливе значення має інформаційна приватність, як характеристика належності інформації певному учаснику. Насамперед ідеться про людину як суб'єкта інформаційно-правових комунікацій та про природу інформаційно-правового статусу людини в інформаційних комунікаціях.

Приватність людини в інформаційних комунікаціях є, насамперед, запорукою її інформаційної захищеності, а тому засновує безпеку людини в інформаційних комунікаціях. Приватність визначає загальний підхід до входження людини в інформаційний простір, оскільки відображає її індивідуалізацію, утворює підставу суб'єктності і саме у такій якості здійснює трансформацію усіх приватно-правових характеристик статусу людини у публічні інформаційно-правові комунікації. Проте не лише у характеристиці інформаційно-правового статусу людини має визначальне значення приватність. Інформаційно-правовий статус будь-якого суб'єкта інформаційних правовідносин має засновуватися на його індивідуальних ознаках. У цьому існує лише одне виключення, яке стосується держави, де індивідуалізація має цілком публічний характер і не залежить від приватності у характеристиці змісту суб'єктності тих інститутів держави, які діють в інформаційно-правових відносинах від її імені.

Звичайно у даному випадку інформаційна приватність розглядається значно ширше, ніж звичне для правової системи США

прайвесі, на чому зосереджуються учені [2, с.77-79]. Однак неможливо не погодитися з поширеними науковими позиціями про те, що приватність в інформаційному сенсі – це право людини на захищеність інформації про особисте і сімейне життя, засноване на положеннях ч.1 ст.32 Конституції України. Подібна позиція повністю відповідає європейській традиції та правовій доктрині США, де розгорнуто учення про прайвесі [3, с.55-60]. Зрозуміло, що протиправне втручання в особисте і сімейне життя людини можливе виключно з використанням відповідної інформації, яка є приватною та захищається комплексом публічно-правових норм і норм цивільного права. Саме у цьому й виявляється комплексність права інформаційної безпеки, що є визнаним у юриспруденції.

В інформаційно-правовому статусі людини приватність є внутрішньою його характеристикою, яка розкриває сутність права людини на інформаційну безпеку. Зовнішнє виявлення суб'єктності людини в інформаційно-правових комунікаціях жодним чином не зосереджується на приватності, оскільки задає відповідний публічно-правовий зміст інформаційно-правових комунікацій.

Без урахування публічності інформаційно-правових комунікацій інформаційна приватність засвідчує участь людини лише у приватних комунікаціях, які у більшості випадків не мають інформаційно-правових ознак, які ідентифікуються інформаційним правом.

Плинність інформаційної приватності є аксіоматично заданою у праві загалом та в інформаційно-правових комунікаціях зокрема. Але така плинність змісту інформаційної приватності жодним чином не відображається на публічно-правовому характері інформаційних комунікацій, що особливо важливо з огляду на публічно визначену можливість захисту права людини на особисту інформацію, на інформаційну приватність.

Невірним є розуміння безумовної переваги і значущості публічно-правових ознак учасників інформаційно-правових комунікацій. Інформаційна приватність є більш важливою у багатьох, якщо не у більшості випадків, коли йдеться про інформацію стосовно конкретної людини або ж конкретно визначеної групи осіб. Навіть за умов публічності таких осіб не вся інформація стосовно них підлягає загальному доступу, а тому захищається правом. Це

якраз кореспондується з положеннями Загальної декларації прав людини [4].

Виникає закономірно питання стосовно того за яких обставин публічність як сутнісна ознака інформаційно-правових комунікацій все ж стає основною та домінує над вимогами приватності. Відповідь на це питання ми можемо дати лише у спосіб розкриття усіх аспектів національної безпеки, де безпека людини поєднується з безпекою суспільства, а отже інших людей, та знаходить свій спільний знаменник у безпеці держави. Єдність усіх ознак права людини на безпеку засвідчує, що приватність поступається місцем публічності стосовно інформації про осіб, які представляють усе суспільство формально і неформально – керівники органів державної влади, керівництво політичними силами, що здатні впливати на формування органів державної влади або ж стосовно осіб, які в силу тих чи інших соціальних обставин становлять загрозу національній безпеці. Проте і тут існує межа – інформація про публічних осіб має бути захищеною до рівня особистої безпеки таких осіб, яка визначає можливість забезпечити свою життєдіяльність і життєдіяльність членів своєї сім'ї.

Публічність, як сутнісна ознака інформаційно-правових комунікацій, не може бути вищою від життя людини, що є натомість найвищою якістю приватності. Якщо ми стверджуємо про життя людини, то розглядаємо не лише безпеку конкретної людини, інформаційна приватність якої захищається правом, але й звертаємося до питання захисту інших людей, життя яких є також важливим, а порушення їхньої приватності, є неприпустимим з позицій права.

Варто розуміти, що національна безпека розглядається не просто як захищеність найбільш важливих національних інтересів, але насамперед як збереження суб'єктності людини, забезпечення стабільності й непорушності її реального правового статусу, правове обґрунтування чому ми знаходимо у праві національної безпеки, а стосовно інформаційно-правового статусу – у праві інформаційної безпеки.

Суб'єктність учасників інформаційних комунікацій та, насамперед, людини має здатність до якісного оновлення лише у стані

інформаційної безпеки, коли захищеність від інформаційних загроз гарантує загалом безпеку життєдіяльності людини. Обмеження інформаційної приватності людини призводить до обмеження суб'єктності в інформаційній сфері, а відтак і суб'єктності загалом. Подібне обмеження може бути предметом дискурсу і практичного вирішення лише у випадку забезпечення права людини на безпеку, коли під такою безпекою розуміється, як зазначалось, не лише безпека однієї людини, а й спільноти, суспільства. Соціетальність загроз для людини, для суспільства обумовлює ситуацію обмеження інформаційної приватності. І навпаки – соціетальна безпека людини стає можливою коли публічно забезпечується інформаційна приватність.

Співвідношення інформаційної приватності та публічності в інформаційно-правових комунікаціях розкривається через положення ст. 29 Загальної декларації прав людини, відповідно до якої кожна людина має обов'язки перед суспільством, в якому тільки й можливий вільний і повний розвиток її особи; при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання та поваги прав і свобод інших і забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві [4].

Залишається актуальною умова обмеження інформаційної приватності – держава позбавляється права на прийняття довільних, необґрунтованих з позицій забезпечення національної безпеки подібних рішень, що суперечить вимогам Конституції України, нормам міжнародного публічного права. Іншою проблемою, яка вирішується у контексті інформаційної приватності, є обов'язок держави забезпечити приватність у спосіб відповідного законодавчого унормування, а також адміністрування, у тому числі щодо реалізації програм діджиталізації (оцифрування інформації).

Отже інформаційна приватність і публічність є сутнісними ознаками інформаційно-правових комунікацій, що утворюють сталу єдність та у своєму існуванні забезпечують не лише інформаційну безпеку людини, суспільства, а й загалом національну безпеку в інформаційній сфері, з орієнтуванням на безпеку людини та суспільства.

Список використаної літератури

1. Селезньова О.М., Юсип Ж.П. Поняття «інформаційні правовідносини»: доктринально-правовий ракурс. *Науковий вісник Ужгородського національного університету*. Серія «Право». – 2017. – Вип.47. – Т.2. – С.21-24.
2. Кардаш А.В. Право на приватність як основоположне право людини. *Науковий вісник Ужгородського національного університету*. Серія «Право». – 2017. – Вип.47. – Т.1. – С.76-80.
3. Серьогін В.О. Секторальний захист інформаційного прайвесі в Сполучених Штатах Америки. *Вісник Харківського національного університету імені В.Н.Каразіна*. Серія «Право». – 2019. – (27) – С.55-63.
4. Загальна декларація прав людини, прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015

Баранов О.А.

доктор юридичних наук,
керівник Науково-дослідного
центру цифрових трансформацій
і права НДІП НАПрНУ

ЦИФРОВА ТРАНСФОРМАЦІЯ ТА КІБЕРБЕЗПЕКА

До початку ХХІ століття сформувалася система змістовно нових цивілізаційних викликів: нераціональне розселення людства на планеті; виснаження планетарних ресурсів; погіршення екології і зміна клімату; погіршення стійкості екосистеми людства; надзвичайно високі темпи соціальних процесів; необхідність великих обсягів інформації та врахування великої кількості об'єктів і суб'єктів для релевантного опису соціальних процесів і прийняття рішень тощо.

Сучасна економічна наука зазнає певних труднощів у розробці інструментарію для створення моделей розвитку глобальної або національної економіки релевантних реальних економічних відносин в соціумі. Оскільки економіка – це основа життєдіяльності людства, то недосконалість її моделей призводило і призводить в стратегічному прогнозуванні та плануванні як до макроекономічних помилок планетарного масштабу, так і до мікроекономічних прорахунків.

«Позапланові» світові, національні та галузеві економічні кризи, неефективні рецепти виходу з них є яскравим свідченням недосконалості методів, способів і механізмів прийняття рішень як при складанні прогнозних моделей економічного розвитку, так і в процесі практичної реалізації цих моделей. У реальному житті корекція або зміна економічних моделей розвитку, як правило, відбувається після факту встановлення наявності кризи або в цілому в економіці, або в окремому її сегменті, або іншими словами, реакція на можливу кризу практично завжди відбувається із запізненням.

Ряд авторів справедливо вважає, що сучасна економічна діяльність людства стає негативним фактором, реально загрозливим перспективам цивілізації на Землі. Це зумовило появу безлічі кон-

куруючих теорій виходу зі сформованого кризового становища [1], які пропонують різні моделі соціальної трансформації.

Факт недосконалості формування та використання моделей розвитку в повній мірі відноситься практично до всіх сегментів соціального життя суспільства: державного управління, економіки, правоохоронної системи, військової сфери, охорони здоров'я, освіти, культури тощо. Тому в останні десятиліття отримала широку популярність ідея проведення всіляких реформ, трансформаційних перетворень в державі та суспільстві.

Одночасно, в світі з кінця 20-го століття широко імплементується в практику ідея інформаційного суспільства та інформатизації. В останні роки багато держав прийняли на найвищому політичному рівні програми цифровізації економіки та інших сфер суспільного життя. Так, наприклад, в цьому році в Євросоюзі закінчується виконання програми розвитку «Європа 2020: стратегія для розумного, стійкого і всеосяжного зростання» (прийнята у 2010 р.) [2]. У цій стратегічній програмі було виділено п'ятий напрямок розвитку – «Цифровий порядок денний» (створення Єдиного цифрового ринка), який став базою для розвитку в інших шести напрямках.

Інформаційне суспільство, комп'ютеризація, інформатизація, цифровізація це різні терміни, але які в своїй суті відображають один і той же процес – процес повсюдного використання надзвичайно цікавих можливостей комп'ютерних і телекомунікаційних технологій, які дозволяють значно підвищити ефективність діяльності в будь-якій сфері соціальної активності. Оскільки критична маса передбачуваних соціальних реформ базується на використанні комп'ютерних і телекомунікаційних технологій, то поряд з терміном «соціальна трансформація» став активно використовуватися термін «цифрова трансформація».

Світові процеси інформатизації (комп'ютеризації) супроводжувалися, правда з деяким запізненням, осмисленням важливості і критичності для них проблем кібербезпеки. У 2003 році з'явилася перша національна стратегія захисту кіберпростору (США) [3]. Після цього в світі розгорнулися широкі дискусії на самих різних рівнях за участю політиків, вчених, експертів і фахівців з різних сфер діяльності про зміст самого терміну «кібербезпека», про

необхідність і шляхи розвитку систем забезпечення кібербезпеки. Понад сім десятків держав з того часу прийняли національні стратегії забезпечення кібербезпеки, в деякі з них – другі і, навіть, треті оновлені редакції.

Сьогодні, створюється враження, що з утворенням у 2019 році постійно діючого Агентства з кібербезпеки Європейського Союзу [4] вже можна констатувати закінчення широких дискусій про актуальність проблеми кібербезпеки. Дійсно, вже ні в кого не виникає сумнівів з приводу необхідності забезпечення кібербезпеки. Але, як і раніше, в сфері загальнодержавних систем кібербезпеки проблемними є: зміст стратегій, визначення цілей побудови і розвитку, формування правових принципів і механізмів функціонування, врахування особливостей сучасного розвитку сфер діяльності в суспільстві, зокрема, за умови їх трансформації, зміст міжнародної кооперації тощо.

Таким чином, актуальність вивчення можливості і необхідності вирішення проблем забезпечення кібербезпеки в умовах широкомасштабних цифрових трансформацій в соціумі не викликає сумнівів. Таке вивчення, перш за все, має базуватися на вивченні діалектичного зв'язку та особливостей змісту соціальної трансформації і цифровий трансформації.

Світова цивілізація, окремі держави, як і будь-які інші динамічні системи (біологічні, технічні або соціальні), розвиваються в умовах постійних зовнішніх і внутрішніх впливів різної природи і різних форм. Зовнішні та внутрішні впливи можуть мати як позитивний, так і негативний характер. **Позитивні впливи** – це ті, які сприяють досягненню мети функціонування динамічної системи (ДС) і, як мінімум, не погіршують якісні характеристики цього функціонування. **Негативні впливи** – це ті, які призводять до істотного погіршення якісних показників функціонування ДСі, навіть, можуть привести до неможливості досягнення мети функціонування (до функціональної загибелі).

Відомо, що самозбереження - це прагнення якомога довше зберегти своє життя, прагнення убезпечити себе від чогось [5]. Отже, властивість **самозбереження системи** – це така властивість, яка спрямована на забезпечення досягнення цілей функціонування шляхом нейтралізації дії негативних впливів.

Тому базовою умовою існування, функціонування і розвитку ДС є наявність у неї такого фундаментальної атрибутивної властивості як самозбереження. Наявність властивості самозбереження забезпечується завдяки функціонуванню спеціальної підсистеми адаптації ДС до змін зовнішніх і внутрішніх впливів. Основне призначення підсистеми адаптації полягає в нейтралізації негативних впливів, що перешкоджають досягненню мети функціонування ДС, і, як мінімум, у збереженні якісних характеристик цього функціонування, а, як максимум, в створенні сприятливих умов для їх підвищення. Нейтралізація реалізації негативних впливів відбувається в результаті певної реакції ДС, ініційованої підсистемою адаптації.

Отже, саме властивість самозбереження, що базується на взаємодії всієї системи і її підсистеми адаптації, лежить в основі всіх процесів еволюції.

Необхідно зауважити, що в ідеалі для забезпечення ефективності самозбереження підсистема адаптації має встигнути ініціювати необхідну реакцію на певний параметр негативного впливу, а ДС – встигнути реалізувати цю реакцію раніше, ніж відбудеться наступна зміна цього параметра негативного впливу. Але, реальні соціальні ДС і їх підсистеми адаптації не можуть виконати зазначену умову тому, що вони мають ряд обмежень щодо ініціювання та реалізації своєчасної реакції на негативні впливи, серед яких основним є час, а також: інформаційні, енергетичні, структурні, просторові, ресурсні, організаційні, управлінські та, навіть, інтелектуальні обмеження. Сказане буде справедливим до тих пір, поки підсистема адаптації не матиме функції прогнозування, що дозволяє заздалегідь, до настання події, пов'язаної з негативними впливами, ініціювати необхідну реакцію.

Таким чином, можна констатувати, що в будь-якому соціальному ДС забезпечення функції самозбереження як основи її існування і розвитку відбувається в умовах наявності протиріччя між необхідністю своєчасно реагувати на негативні впливи і об'єктивним існуванням обмежень для забезпечення необхідної якості такого реагування.

Одним з найбільш ефективних шляхів вирішення зазначеного вище протиріччя є перетворення (трансформація) ДС з метою мі-

німізації або повного виключення обмежень в забезпеченні необхідної якості реагування на певні негативні впливи.

Отже, з метою забезпечення ефективності властивості самозбереження – ДС і її підсистема адаптації мають бути здатні виконувати такі завдання:

- ідентифікація впливів;
- спостереження і прогнозування їх розвитку;
- аналіз дії впливів на показники функціонування ДС;
- синтез «пропозицій» по вдосконаленню ДС, зокрема, зі зміни правил поведінки (вдосконалення колишніх або створення нових, в тому числі норм права) для мінімізації наслідків негативних впливів;
- формування «пропозицій» про шляхи, методи, способи і засоби забезпечення вдосконалення (зміни) ДС, зокрема, формування вдосконалених правил поведінки;
- аналіз дії негативних впливів на показники функціонування вдосконаленої ДС;
- корекція (при необхідності) попередніх «пропозицій» щодо вдосконалення ДС.

В останні роки для позначення процесів змін, модернізації, вдосконалення або реформування широко використовується термін «соціальна трансформація», метою якої оголошують забезпечення підвищення ефективності функціонування суспільства або окремих його частин.

На наш погляд, *соціальна трансформація це перетворення або корекція мети, структури і функцій всього суспільства або його окремих частин, а також методів, способів і механізмів їх реалізації, для забезпечення адаптації до суттєвих змін внутрішніх та зовнішніх умов його функціонування, які є загрозою ефективності його подальшого розвитку.*

Більшість дослідників і представників експертного середовища вважають, що один з панівних методів соціальної трансформації – це техніко-економічний метод, базовим критерієм якого є ефективність. Історично показано, що техніко-економічні методи трансформації реалізуються через промислові (технологічні) революції, які сприймають як революційні зміни в продуктивних силах суспільства і в організації його діяльності в найширшому сенсі [6].

Промислова революція завжди була відповіддю на цивілізаційний виклик, обумовлений виникненням системного протиріччя між необхідністю забезпечення самозбереження цивілізації та між наявністю цивілізаційних системних обмежень по нейтралізації дії негативних впливів, що загрожують самому існуванню цивілізації.

В якості причин нових цивілізаційних викликів, які сформувалися до початку 21 століття, можна назвати наступні:

- надзвичайно високі темпи соціальних процесів;
- необхідність наявності великих обсягів інформації та врахування великої кількості об'єктів і суб'єктів для релевантного опису соціальних процесів;
- необхідність приймати рішення в режимі реального часу;
- обмеженість когнітивних здібностей людини для прийняття рішень адекватних сучасному стану соціальних процесів, внутрішніх і зовнішніх впливів;
- обмеженість фізичних і біологічних можливостей людини для реалізації великої кількості сучасних та майбутніх видів соціальної діяльності.

Відповіддю на сучасні цивілізаційні виклики стала четверта промислова революція, до основних досягнень якої відносять технології Інтернету речей, Індустрії 4.0, штучного інтелекту, робототехніки, великих даних, хмарних обчислень, нано- та біотехнологій, генної інженерії, електронних комунікацій тощо. Спільне застосування цих досягнень створює надпотужний синергетичний вплив на підвищення ефективності будь-якої діяльності, різку економію ресурсів, значне поліпшення якості життя людей тощо [7].

Впровадження зазначених вище досягнень вимагає проведення певної соціальної трансформації як в межах окремої країни або групи країн, так в межах всієї цивілізації. Це пояснюється тим, що синергія цивілізаційного ефекту від нових технологій збільшується в геометричній прогресії за умови їх різкого масштабування на основі широкого використання інформаційних комп'ютерних технологій (цифрових технологій) [8, 9].

Будемо вважати, що **цифрова трансформація** – це соціальна трансформація, яка відбувається на основі максимального використання цифрових технологій таких як: Інтернет речей, Індустрія

4.0, штучний інтелект, робототехніка, великі дані, хмарні обчислення, електронні комунікації, а також, нано- та біотехнологій, генної інженерії тощо.

Виходячи з аналізу дефініцій і внутрішнього сенсу соціальної трансформації і цифровий трансформації можна зробити висновок про діалектику їх зв'язку як категорій змісту і форми. Зміст - це соціальна трансформація, яка полягає в зміні або перетворенні соціуму, іноді, корінному. Використання цифрових технологій означає особливу форму реалізації певної соціальної трансформації - цифрову трансформацію. При цьому може мати місце відомі наслідки діалектики зв'язку категорій змісту і форми. Конкретний зміст соціальної трансформації може детермінувати вибір форм (способів, засобів і механізмів) цифровий трансформації. У свою чергу реалізація конкретних форм цифрової трансформації може привести до необхідності проведення певної соціальної трансформації або зміни змісту соціальної трансформації, що проводиться.

У загальному випадку, і соціальна трансформація, і цифрова трансформація неминуче призводять до:

- зміни змісту і складу системи суспільних відносин, які охоплюються ними, а іноді, навіть до появи нових груп суспільних відносин;
- зміни парадигми функціонування держави, соціуму і його окремих сегментів, життєдіяльності окремих людей;
- переходу до інноваційних бізнес-процесів і бізнес-моделей тощо.

Тому будь-які трансформації безперечно мають наслідком необхідність корекції або навіть зміни відповідної соціальної моделі суспільства і будь-яких інших видів моделей соціуму (економічної, інформаційної, правової тощо). А це неминуче тягне за собою і зміну правової моделі відповідної якоїсь конкретної соціальної моделі суспільства.

Як правило, застосування правової моделі регулювання суспільних відносин, яка базується на чинному законодавстві, до нової соціальної моделі суспільства призводить до виникнення правових проблем. Крім загальних підстав для виникнення цих проблем, необхідно враховувати ще й те, що застосування цифрових техно-

логій, як правило, стає каталізатором появи нових за змістом суспільних відносин або появи особливостей реалізації вже відомих суспільних відносин. Отже, соціальна або цифрова трансформації, оскільки вони є джерелом виникнення правових проблем, повинні супроводжуватися відповідними змінами системи законодавства, які в свою чергу повинні бути обґрунтовані відповідними науковими правовими дослідженнями. Немаловажну частину цих правових проблем складають проблеми пов'язані з кібербезпекою.

Таким чином, до питання виникнення і вирішення правових проблем, в тому числі пов'язаних з кібербезпекою, необхідно підходити з системних, інтегративних позицій вивчення цілей, завдань і наслідків як соціальної трансформації, так і цифровий трансформації суспільства.

Література.

1. А Бобрышев, М Тарабрин, К Тарабрин, 'Формирование бизнес-модели устойчивой производственной компании' (ГБОУ Московская академия рынка труда и информационных технологий, 04 июля 2015) <http://www.cfin.ru/management/controllers/business_model.shtml> дата звернення 20 травня 2020.
2. European Commission, 2010. Europe 2020: A strategy for smart, sustainable and inclusive growth. COM(2010) 2020 final <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:2020:FIN:EN:PDF>>
3. The national strategy to secure cyberspace (Washington 2003) 60. <www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf>
4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) <<http://data.europa.eu/eli/reg/2019/881/oj>> дата звернення 20 травня 2020.
5. Толковый словарь русского языка / Под ред. Д.Н. Ушакова. – М.: Гос. ин-т „Сов. энцикл.”; ОГИЗ; Гос. изд-во иностр. и нац. слов., 1935-1940. (4 т.) <<https://ushakovdictionary.ru/word.php?wordid=67702>> дата звернення 20 травня 2020.

6. С.С. Буддыгин Концепция промышленной революции: от появления до наших дней Вестник Томского государственного университета. 2017. № 420. С. 91–95. DOI: 10.17223/15617793/420/12 <<https://cyberleninka.ru/article/n/kontseptsiya-promyshlennoy-revolutsii-ot-poyavleniya-do-nashih-dney>> дата звернення 20 травня 2020.

7. LIAO, Yongxin et al. The impact of the fourth industrial revolution: a cross-country/region comparison. Prod. [online]. 2018, vol.28 [cited 2020-05-03], e20180061. Available from: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0103-65132018000100401&lng=en&nrm=iso> дата звернення 20 травня 2020. . Epub Jan 15, 2018.

8. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services (World Economic Fo-rum 2015) 39. <http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf> дата звернення 20 травня 2020.

9. The Future of Jobs. Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution (The World Economic Forum 2016) 157. <www3.weforum.org/docs/WEF_Future_of_Jobs.pdf> дата звернення 20 травня 2020.

Дзьобань О.П.

доктор філософських наук,
професор, головний науковий
співробітник
НДІ інформатики і права Національ-
ної академії правових наук України

АДАПТАЦІЯ ЛЮДИНИ ДО УМОВ СУЧАСНОГО ІНФОРМАЦІЙНОГО СЕРЕДОВИЩА: БЕЗПЕКОВІ ПРОБЛЕМИ

У сучасному соціумі поширення інформаційних технологій супроводжується віртуалізацією всіх сфер людського життя, перетворившись з простої технології в інформаційно-комунікативне середовище. На сьогоднішній день розширення його впливу відбувається у двох основних взаємопов'язаних напрямках: збільшення впливу віртуальності на світ реальний і віртуалізація самої реальності, які проявляються у надбанні віртуального статусу усіма сферами світу людини й соціокультурної реальності. Технічні засоби й інформаційні прийоми організації віртуальної реальності здатні кардинально змінити характер і змісти життєдіяльності як людини, так і соціуму в цілому.

Масштабність проникнення віртуальної реальності у соціальне життя дає підставу вести мову про «віртуалізацію» суспільства, яка змінює спосіб життя людей, роблячи його синтетичним, посилюючи прагнення потрапити в нові її шари. Віртуальність є тотальною й безмежною, вона охоплює все більшу кількість сфер суспільного життя. У віртуальній реальності поступово зникають просторові та часові розмежування, стираються міждержавні кордони, пропагуються нові цінності, моделі поведінки, світоглядні стереотипи. Феномен віртуалізації життєвого простору людини та суспільства характеризує принципово новий тип символічного існування людини.

Однією з базисних характеристик інформаційного суспільства є формування нової людини – «людини інформаційної». У даній характеристиці важливими стають наступні визначальні моменти.

По-перше, значущим є те, якою повинна бути особистість в умовах інформатизації. В умовах розгортання інформатизації кожне з діалектично взаємозв'язаних начал людини – фізичне, психічне й соціальне – вимагає спеціального урахування, оскільки лише у цьому випадку нові можливості інформаційного суспільства можуть бути повною мірою використані для розвитку людини. Без урахування специфіки цих начал людини, інформатизація чревата негативними суспільними наслідками.

Є усі підстави виділити наступні основні соціальні проблеми адаптації людини до мінливих умов інформаційного суспільства:

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

Впливами на особистість можуть виступати:

- цілеспрямований інформаційний тиск з метою зміни світогляду, політичних поглядів і морально-психологічного стану людей;
- розповсюдження недостовірної, спотвореної, неповної інформації;
- використання неадекватного сприйняття людьми достовірної інформації. Інформаційні впливи є небезпечними або корисними не стільки самі по собі, скільки тим, що управляють могутніми речовинно-енергетичними процесами. Суть впливу інформації якраз і полягає в її здатності контролювати речовинно-енергетичні процеси, параметри яких є на порядок вищими за саму інформацію;
- комп'ютерна злочинність, віруси. Спроба творців вірусів, як правило, молодих людей реалізувати себе у вірусотворчості пов'язана низкою причин: бажанням самостверджуватися, «прогриміти», а також відсутністю усвідомлених життєвих цілей.

Підкреслимо, що в сучасних умовах змінюється не тільки технологічна база й інформаційно-технологічні можливості людини, але

й сама людина, її самосвідомість. Сучасна людина стає немислимою без інформаційних технологій, які здійснюють величезний вплив на все її існування – як біологічне, так і соціальне. Предметом дискусій стає лише те, що несуть ці зміни.

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

Наскільки ширшою є сфера застосування технічного, настільки менше аспектів людської діяльності залишаються незалежними від неї.

Отже, сьогодні на перший план виходить проблема безпечної адаптації людини в сучасному інформаційному середовищі. Інформаційне середовище, стаючи все більш важливою і невід'ємною частиною навколишнього середовища, пред'являє до людини зростаючі адаптивні вимоги. Людство було вимушене адаптуватися до природного й штучно створеного інформаційного середовища протягом усього свого розвитку, проте, життя сучасної людини визначається новими реаліями, новими екологічними й соціальними обставинами.

Створення сучасного світового інформаційного простору поступово висуває нові вимоги перед людиною як духовно-суспіль-

ною істотою, здатною приймати виклики інформаційної цивілізації і нести відповідальність за власні дії та їх наслідки.

Розвиток комп'ютерних мереж веде до формування специфічних віртуальних співтовариств, при цьому спостерігається широка соціальна й культурна диференціація. Важливим антропологічним аспектом стає проблема відчуження, коли пасивне споживання інформації формує жорсткість мислення, позбавляє людей безпосереднього спілкування один з одним, звужує персональний простір, призводить до втрати міжособового спілкування.

Головний вплив на трансформацію людини здійснюють інформаційні й комунікаційні технології, за якими слідують біотехнології, які вже можуть змінювати нас самих, а не характер наших дій.

Сучасна наука і техніка, зберігаючи загальну установку на перетворення об'єктивного світу, втягують в орбіту людської діяльності принципово нові типи об'єктів, які змінюють тип раціональності й характер діяльності, що реалізується у виробничих і соціальних технологіях. Йдеться про складні системи, що саморозвиваються, серед яких головне місце займають людинорозмірні, які включають у себе людину як свій особливий компонент. При вивченні людинорозмірних об'єктів пошук істини виявляється пов'язаним з визначенням можливих напрямів перетворення такого об'єкта, що безпосередньо торкається гуманістичних цінностей. Людина реагує на зміну зовнішньої обстановки тим, що змінюється сама, передусім психічно. Вона постає перед вибором, який базується на усвідомленні як негативних наслідків «занурення» у простір інформаційного суспільства, так і конструктивних, позитивних можливостей, зумовлених благами такого суспільства. Проте, інтеграція людства й інформаційних технологій здебільшого призводить до негативних наслідків.

Таким чином, нова мережева форма організації сприяє становленню нової «мережевої людини», яка характеризується низкою відмінностей. Перша відмінність нової «мережевої» людини – середовище взаємодії. Людина живе в такому комунікаційному просторі, відмінними рисами якого є відсутність меж, а взаємини відрізняються цілою низкою нових рис і характеристик, які виникають на основі горизонтальних зв'язків. Другою важливою межею в «комп'ютерній» людині опиняється трансформація простору й часу, яка стала також

результатом інформаційної модернізації й розвитку комунікацій. Третьою характеристикою нової «мережевої» людини є втрата ідентичності. Культура «віртуальної реальності» стає фундаментальною четвертою межею нової «мережевої» людини. П'ятою відмінністю є гендерні зміни. Основною суперечністю мережевого суспільства, що формується, і людини, є суперечність між глобалізацією світу й ідентичністю конкретної людини, між віртуальним простором і присутністю в ньому малих етнічних і культурних груп, що претендують на збереження ідентичності.

Людина потенційно готова жити і працювати в якісно новому інформаційному середовищі, адекватно сприймати його реалії і, більше того, успішно розвивати його. Таким чином, це змінює не тільки умови життя людини, але і її саму. Проте, ці зміни носять суперечливий, часом навіть небезпечний характер, що пов'язано з багатьма вельми різноплановими чинниками, наприклад, з необхідністю виділення значних ресурсів суспільства, з неминучою і нерідко хворобливою ломкою різних структур (соціально-економічних, виробничо-технологічних, культурних, чисто інформаційних тощо), з труднощами культурно-психологічної адаптації людини до нетрадиційних інформаційних засобів і технологій. Коротше кажучи, цей процес не можна представляти як суто позитивне явище, без недоліків, витрат і небажаних наслідків.

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

Багато дослідників заговорили про виникнення людини нової культури, яка демонструє залежність трансформації свідомості від використання абсолютно нового для людської руки інструменту – кнопки. Адже користувач персонального комп'ютера проводить за

ним стільки часу і так швидко звикає до механізмів роботи, що можна стверджувати, що кнопка стає новим культурним артефактом.

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

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

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

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

Беланюк М.В.

кандидат юридичних наук,
учений секретар НДПП НАПрН
України

ПРАВА ЛЮДИНИ В ІНТЕРНЕТ

Право на свободу інформації у міжнародному праві визнано фундаментальним правом людини і головним критерієм всіх свобод, про що було проголошено на Першій сесії Генеральної Асамблеї ООН у далекому 1946 році у Резолюції 59 (I) «Скликання міжнародної конференції з питань свободи інформації» [1; 19]. Згодом ця концепція знайшла відображення у Загальній декларації прав людини[2], Міжнародному пакті про громадянські та політичні права[3] та ін. міжнародних документах, основний акцент у яких був зроблений на тому, що право збирати, отримувати і поширювати інформацію, реалізується *«незалежно від державних кордонів»*. Згідно з Конвенцією про захист прав людини і основних свобод, свобода вираження поглядів і отримання інформації є практично необмеженою [4].

За національним законодавством право на свободу інформації гарантовано статтею 34 Конституції України *«кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб - на свій вибір»* [5]. Виключенням для обмеження цього права є: в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя. Крім Конституції право доступу до інформації регулюється законами України «Про Інформацію»[6], «Про доступ до публічної інформації»[7], «Про захист інформації в інформаційно-телекомунікаційних системах» [8], «Про друковані засоби масової інформації (пресу) в Україні»[9] та ін.

У резолюції Ради ООН з прав людини від 5 липня 2012 р. наголошувалося на тому, що ті ж права, які мають люди в режимі офлайн,

також повинні бути захищені в Інтернеті. Для забезпечення прав людини на свободу вираження своїх поглядів та переконань усі люди повинні мати доступ до мережі Інтернет, а держава має *«заохочувати та полегшувати доступ до Інтернету та міжнародного співробітництва, спрямованого на розвиток засобів масової інформації та засобів зв'язку у всіх країнах»*[10]. Крім того зазначалося, що Інтернет –важливий інструмент розвитку та реалізації прав людини і Рада й надалі буде опікуватися питаннями пропаганди, захисту та реалізації прав людини, включно з правом на свободу вираження поглядів в Інтернеті [10].

Оскільки саме Інтернет в сучасному світі виконує функцію ката-лізатора для здійснення всіх прав людини і є потужним фактором соціального, освітнього і культурного розвитку та головним дже-релом інформації у сучасному суспільстві, незалежно від кордонів, **зупинимось на розгляді основних прав людини, пов'язаних з ви-користанням Інтернету, так звані “Цифрові права”, які у захід-них країнах розуміються як «доступ» і «недискримінація» - віль-ний доступ, свобода вираження поглядів та приватність онлайн, англ. - «digital rights».**

Отже основним цифровим правом людини є право на доступ до Інтернету, що передбачає можливість вільного та безпечного користування цією мережею. Це право забезпечується шляхом за-борони необґрунтованого обмеження доступу до Інтернету та зобов'язання держав вживати заходів для забезпечення максималь-ного доступу своїх громадян до мережі.

Умовами для повноцінної реалізації цього права громадянами є також доступ до інформації про технології та цифрова грамотність – можливість отримувати знання та навички з використання Інтер-нету для задоволення своїх потреб. Право на доступ до інтернету має базуватися на принципах інклюзивності, недискримінації, **ме-режевій нейтральності, безпеці та якості надання послуг** [11].

Кожен має право вільно висловлювати свої погляди, шукати, от-римувати та поширювати інформацію онлайн. Реалізація права на свободу вираження поглядів передбачає, що нікого не можна при-мушувати до дій чи висловлювань проти своїх переконань. Право шукати й отримувати інформацію означає не лише те, що держава

не повинна перешкоджати людині шукати інформацію онлайн, але й має сприяти доступу до такої інформації. Право поширювати інформацію означає, що особа може вільно висловлюватись, навіть якщо її слова можуть образити людину, але лише за умови, що вони не порушують закон та прав і свобод інших людей. Це право також передбачає можливість використання анонімності або псевдоніму задля своєї безпеки, оскільки доступ до Інтернету, крім переваг, пов'язаний із можливими ризиками і загрозами для людини (наси́льство, кібербу́лінг, кібербо́мінг і т.д.). Свобода вираження поглядів має бути вільною від цензури, але разом з тим покладає обов'язки не порушувати закон та поважати права інших людей.

Задля забезпечення права на приватність та захист персональних даних в Інтернет, країни мають адаптувати своє законодавство до міжнародних стандартів та критеріїв, а саме: збирання та обробка персональних даних має здійснюватися за згодою або з інших підстав, чітко визначених законом; персональні дані мають збиратися в обсязі, що відповідає меті обробки, яка водночас має бути законною та виправданою; особа повинна бути належним чином поінформована про обробку своїх персональних даних та її мету; персональні дані не можуть поширюватися чи оброблятися для інших, ніж було визначено і погоджено, цілей; безпечне зберігання персональних даних; право отримати інформацію про обробку та свої персональні дані; право вимагати виправлення або видалення своїх персональних даних; право на відшкодування у разі порушення.

Наразі в Україні не створено ефективної системи захисту персональних даних. Законодавство України має відповідати міжнародним стандартам, хоча б мінімальним критеріям щодо контролю користувачів над власними даними. Для цього в Україні мав бути створений ефективний наглядовий орган у сфері захисту персональних даних. Уповноваженим органом з питань захисту персональних даних в Україні визначено Уповноваженого Верховної Ради України з прав людини. Слід зазначити, що покладання функції парламентського контролю та центрального органу виконавчої влади на Уповноваженого Верховної Ради України з прав людини не відповідає вимогам Конституції України і законодавства ЄС.

Право на захист приватності передбачає не тільки захист від посягання на репутацію особи через поширення недостовірної інформації, але й шляхом невтручання у таємницю кореспонденції та електронних комунікацій. Забезпечення цього права можливе за допомогою шифрування інформації та повідомлень онлайн та через обмеження неконтрольованого доступу правоохоронних органів до інтернет-мереж.

Як і в реальному житті, людина має бути убезпечена від злочинних посягань в Інтернеті (фізичного та психологічного насильства, домагань, дискримінації тощо). Механізм забезпечення свободи та особистої безпеки в Інтернеті повинен відповідати викликам та загрозам та має постійно вдосконалюватись для юридичних гарантій захисту людини в онлайн-середовищі. Водночас держава має сприяти розвитку та функціонуванню безпечних інтернет-технологій, поряд із захистом технічного функціонування Інтернету від шкідливих сервісів. Відповідно до Будапештської конвенції про кіберзлочинність [12] користувачі Інтернету мають бути захищеними від використання шкідливих кодів та надсилання великих обсягів електронних листів з метою блокування комунікаційних функцій системи.

Інтернет спільноти в сучасному світі – це важлива складова участі громадян в суспільному житті країни. За допомогою Інтернету забезпечується право людини на мирні зібрання, що значно пришвидшує вирішення важливих державних справ. Задля забезпечення цього права громадяни повинні мати свободу обирати та використовувати будь-які сервіси чи веб-сайти для створення, приєднання, мобілізації та участі в соціальних групах. Це право охоплює також право на мирний онлайн-протест, на використання без необґрунтованого втручання всіх доступних сервісів та послуг електронної демократії, включно з правом подання електронних петицій.

Існування **права на цифрове самовизначення або права відключатися від онлайн на сьогодні є** предметом теоретичних дискусій. Уперше про право відключатися почали говорити в аспекті трудових прав, з урахуванням створюваних ситуацій, коли робочі питання необхідно було вирішувати онлайн у позаробочий час. Все

більше фахівців звертається до думки, що, будь-який громадянин повинен мати доступ до головних державних сервісів і не зазнавати дискримінації незалежно від своєї віртуальної активності або її відсутності.

Там, де є права там є і їх порушення. Результати моніторингу порушення цифрових прав в Україні за квітень-вересень 2019 року [13]:

- 16 рішень у справах, які стосуються порушення обмежень щодо ведення передвиборної агітації, пов'язаної з поширенням користувачами соціальних мереж фотографій бюлетенів із результатами свого волевиявлення у той час, коли ще тривало голосування на виборчих дільницях;

- 4 порушення права на свободу вираження поглядів (напад на журналістів і онлайн видань та/або блогерів, позов про захист честі, гідності, ділової репутації, пов'язаного із поширенням інформації у соціальній мережі, порушення авторського права в Інтернет);

- 6 порушень права на приватність та захист даних (витік персональних даних журналістів, свідоме поширення персональних даних, продаж баз даних, шахрайство з банківськими персональними даними користувачів, злам персональних сторінок у соціальних мережах тощо);

- 9 порушень цифрових прав індивідуального характеру (7 порушень права на свободу вираження поглядів, 2 – права на приватне життя та захист даних);

- 3 загрози для свободи слова в Інтернеті в Україні.

З урахуванням зазначеного приходимо до висновків, що в Україні ефективної системи захисту цифрових прав людини не створено. Насамперед існує проблема імплементації норм законодавства ЄС в національне законодавство та відсутні ефективні цифрові системи технічного захисту персональних даних в Інтернет.

В інформаційному суспільстві, яке створило і розвиває людство, Інтернет є одним з найпотужніших джерел знання і усі повинні мати можливість бути активними його учасниками. Ті права, які нещодавно були офлайн дедалі швидше переходять у права онлайн. Так, до **цифрових прав вже можна зарахувати право на освіту, право на працю, на підприємницьку діяльність, права користувачів, право на охорону здоров'я, культурні і інші пра-**

ва. З подальшим розвитком інформаційних технологій цифровий вимір прав людини дедалі збільшуватиметься, що потребуватиме ефективних засобів їх правового та технічного захисту, а також удосконалення механізму міжнародного унормування.

Список використаної літератури

1. Шевердяев С. Н. Право на доступ к информации в России: проблемы теории и законодательства // Журналистика и право – М.: Инс-т проблем информ. права, 2004. – Вып. 35. – С. 18–23.

2. Загальна декларація прав людини. ООН; Декларація, Міжнародний документ від 10.12.1948 URL: https://zakon.rada.gov.ua/laws/show/995_015(дата звернення: 15.05.2020).

3. Міжнародний пакт про громадянські і політичні права. ООН; Пакт, Міжнародний документ від 16.12.1966 : URL: https://zakon.rada.gov.ua/laws/show/995_043(дата звернення: 18.05.2020).

4. Конвенція про захист прав людини і основоположних свобод. Рада Європи; Конвенція, Міжнародний документ від 04.11.1950 URL: https://zakon.rada.gov.ua/laws/show/995_004(дата звернення: 18.05.2020).

5. Конституція України. Верховна Рада України; Конституція України, Конституція, Закон від 28.06.1996 № 254к/96-ВР: URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>(дата звернення: 18.05.2020).

6. Про інформацію. Закон України від 02.10.1992 № 2657-XII : URL: <https://zakon.rada.gov.ua/laws/show/2657-12>(дата звернення: 18.05.2020).

7. Про доступ до публічної інформації. Закон України від 13.01.2011 № 2939-VI : URL: <https://zakon.rada.gov.ua/laws/show/2939-17>(дата звернення: 18.05.2020).

8. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР: URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80>(дата звернення: 18.05.2020).

9. Про друковані засоби масової інформації (пресу) в Україні. Закон України від 16.11.1992 № 2782-XII: URL: <https://zakon.rada.gov.ua/laws/show/2782-12>(дата звернення: 18.05.2020).

10. Генеральна Асамблея Ради ООН з прав людини. Резолюція «Про сприяння, захист та здійснення прав людини в Інтернеті»: URL: <https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx>, (дата звернення: 18.05.2020).

11. Володовська В. Заборони та свободи в інтернеті: як виглядатиме Декларація цифрових прав людини: URL: https://zmina.info/articles/zaboroni_ta_svbodi_v_interneti_jiak_vigljadati_time_deklaracija_cifrovih_prav_ljudini/ (дата звернення: 18.05.2020).

12. Конвенція про кіберзлочинність. Рада Європи; Конвенція, Міжнародний документ від 23.11.2001 URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 15.05.2020)

13. Гололобова Є., Міна А. Цифрові права українців або Декларація цифрових прав людини URL: <https://www.businesslaw.org.ua/digital-rights-t/> (дата звернення: 18.05.2020).

Арістова І.В.,

докторка юридичних наук,
професорка, завідувачка кафедри
адміністративного
та інформаційного права
Сумського національного аграрного
університету

ОХОРОНА ПРАВА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ В УКРАЇНІ

Загальноновизнано, що майбутнє світу та й України в цілому ґрунтується на цифрових технологіях, поштовх яким дає, серед іншого, й сучасна цифрова економіка. Актуальність цього феномену зазначено й на міжнародному рівні, коли питання цифрової економіки вперше було внесено у порядок денний групи G20 на саміті в Анталії у 2015р. та визнано, що ми живемо в епоху економіки Інтернету [1]. Тому, не випадково, що у Концепції розвитку цифрової економіки та суспільства України на 2018–2020 рр. акцентовано увагу на тому, що «важливими для розвитку цифрової економіки є м'які цифрові інфраструктури, які не повинні залишатися поза увагою, зокрема й інфраструктура блокчейн» [2]. Однією з рушійних сил розвитку цивілізації є творча інтелектуальна діяльність. Країни з ринковою економікою давно усвідомили значення використання і належної охорони результатів творчої діяльності, об'єднаних у понятті «інтелектуальна власність», для темпів соціального та економічного розвитку [3, с. 384]. Важливість розв'язання цього завдання закріплено в Угоді про асоціацію України з Європейським Союзом [4].

У роботі відстоюється позиція, що цифрова економіка постає однією із ознак інформаційного суспільства, яке у своєму розвитку проходить декілька етапів [5, с. 3]. Безумовно, в нових умовах виникає об'єктивна потреба у переосмисленні ролі права, напрямків розвитку галузей права та їх взаємодії. Важливо, що державна підтримка зазначеної позиції знайшла своє втілення, наприклад, у Рекомендаціях парламентських слухань на тему: Законодавче забезпечення розвитку інформаційного суспільства в Україні [6].

Мета роботи полягає у визначенні особливостей використання правових засобів інформаційного права та права інтелектуальної власності, а також інструментів цифрової економіки для врегулювання суспільних відносин у сфері інтелектуальної власності в Україні. Відповідно до вимог методології наукового дослідження, для досягнення зазначеної мети висувається та перевіряється наступна наукова гіпотеза: необхідною умовою належного забезпечення права інтелектуальної власності в умовах розбудови суспільства знань в Україні постає комплексне використання правових засобів інформаційного права й права інтелектуальної власності, а також інструментів цифрової економіки.

Перед перевіркою зазначеної гіпотези вважаємо за доцільне визначитися із основними поняттями правових засобів та інструментів цифрової економіки. У роботі акцентовано увагу на необхідності розуміння змісту та структури поняття правові засоби (засоби правового регулювання). Це – «правові явища, що призначені для правового упорядкування суспільних відносин, оптимального вирішення соціальних завдань, досягнення суб'єктами правовідносин приватних та публічних цілей [7, с. 284, 285]. Варто підкреслити, що поняття «засіб» містить у собі як інструментарій (засоби - встановлення), так і технології (засоби - дії). До першої складової належать, наприклад, зобов'язання, дозволи, заборони, заохочення, рекомендації, покарання, пільги, норми права, принципи права та ін. Друга складова правових засобів включає акти реалізації права, акти застосування права і всі процеси юридичної діяльності [7, с. 285]. До речі, наведені види правових засобів було сгруповано за критерієм регулятивної активності. Водночас, за критерієм галузевої приналежності правові засоби поділяються на конституційні, адміністративні, цивільні, інформаційні тощо. Вважаємо за доцільне зазначити, що у процесі перевірки висунутої наукової гіпотези будуть використовуватися елементи наведених груп правових засобів.

Аналіз літератури, зокрема монографії [8], дозволив встановити, що інструментами цифрової економіки постають блокчейн, токен блокчейну, цифровий актив та смарт-контракт. Блокчейн – це структурована база даних, «ланцюжок блоків», де кожен блокпов'я-

заний з попереднім та містить в собі набір записів (інформації про події, людей, об'єкти, транзакції, серійні номери, видані кредити та ін. [9]. Основними принципами функціонування, що закладені у технології блокчейн, є абсолютна прозорість, «довірчий» характер системи, відкритість та захищеність даних користувачів, доступність до історії транзакції усіх учасників, розподіленість реєстру [8, с. 14].

Вважаємо за необхідне нагадати, що : 1) токен блокчейну – це одиниця обліку блокчейну[8, с. 47].; 2) цифровий актив – це інформаційний ресурс, похідний від права на цінність і такий, що обертається в розподіленому реєстрі у вигляді унікального ідентифікатора [8, с. 351].; 3) смарт-контракт – це контракт на даних розподіленого реєстру блокчейн, де використовується принцип «якщо..., то», тобто, умова прямо визначена у контракті [10, с. 102].; 4) комплексівластивості токenu блокчейнузводяться до виконанняоднієї важливої функції – допуску до інформаційного ресурсу, який, у свою чергу, надає доступ до певного комплексу прав на цінність, під якими прийнято розуміти майно, майнові та немайнові права, цінні папери, послуги, роботи, цифрові активи тощо [8, с. 73]. Тобто, виникає реальна можливість охорони різноманітних прав людини за допомогою технології блокчейн та її інструментів. Будемо вважати таку охорону технологічною. На нашу думку, наступні положення нашої роботи сприятимуть більшому усвідомленню такої позиції.

Дійсно, проведені дослідження сприяли усвідомленню того, що потенціал природи технології блокчейн здатен самостійно сприяти всебічному формуванню довірчих відносин у суспільстві, охоплюючи такі додаткові характеристики як прозорість та фактичність, а також гарантуванню принципу рівності, що дійсно є дуже актуальним для суспільства на сьогоднішній день, особливо у зв'язку із необхідністю охорони прав людини. Як показали дослідження [8, с. 293], то надзвичайно ефективно блокчейн може бути застосований у сфері прав інтелектуальної власності, що і було перевірено під час нашого дослідження. Водночас, проведені дослідження дозволили дійти висновку, що, використовуючи смарт-контракти, також можна спростити діяльність у багатьох сферах життя, в тому

числі у юриспруденції, а саме, під час охорони права інтелектуальної власності [10, с. 101-110]. Наприклад, з'ясовано, що, з огляду на властивості цифрового активу у розподіленому реєстрі, реєстрація об'єктів права інтелектуальної власності в блокчейні у вигляді інформаційних ресурсів («оцифровування») дає можливість власникам авторських прав уникнути плагіату, «піратського» розповсюдження, надає контролінг за легальністю розповсюдження результатів творчої та наукової діяльності (музичних творів, статей, наукових досліджень тощо) через обертання цифрових активів, у які закладено ці об'єкти прав інтелектуальної власності [8, с. 294]. І це, на наш погляд, є наступним напрямом перспективного впровадження технології блокчейн, задля технологічної охорони права інтелектуальної власності. Водночас, встановлено, що і під час впровадження ідеї смарт-контрактів на базі розподіленого реєстру, і під час вирішення проблеми ліквідації анонімності користувачів блокчейну виникає потреба у комплексному використанні інструментів цифрової економіки та правових засобів інформаційного права та права інтелектуальної власності.

У роботі усвідомлено, що існують різні підходи до розуміння поняття права інтелектуальної власності (далі – ІВ). Пропонуємо дотримуватися наступної дефініції: «Інтелектуальна власність – термін, який склався історично, є умовним та має тільки термінологічну схожість із правом власності у його традиційному сприйманні і повинен розумітися як сукупність виключних прав особистого і майнового характеру на результати інтелектуальної діяльності», котрі не є правами власника... Відповідно до такого бачення право на об'єкти інтелектуальної власності складаються з двох правомочностей: право забороняти та/чи дозволяти їх використання третім особам» [10, с. 218].

Вважаємо за необхідне зазначити, що ґрунтовно питання правової охорони права інтелектуальної власності розкрито у [11, с. 255-288], з відповідними посиланнями на науковців та наведенням власних обґрунтованих висновків.

Ґрунтуючись на розумінні інтелектуальної власності як сукупності виключних прав особистого і майнового характеру, а права інтелектуальної власності – у об'єктивному та суб'єктивному зна-

ченні, встановлено та проаналізовано нормативно-правові акти (національні та міжнародні), що постають фундаментом правової охорони об'єктів права ІВ. Акцентування уваги на охороні об'єктів авторського і патентного права дозволило встановити, що відмінність цих об'єктів зумовлюється особливостями їх правової охорони, які було зазначено у роботі [11, с. 255-288]. Дійшли висновку, що правова охорона об'єктів ІВ: а) здійснюється за допомогою надання їх створювачу виключних прав; б) побудована на принципі поєднання інтересів створювача інтелектуального продукту та інтересів суспільства. Акцентовано увагу на значенні інформації у правовій охороні ІВ.

Йдеться, наприклад, про розкриття особливостей правової охорони інтересів учасників суспільних відносин в ІТ-компаніях, інтелектуальними продуктами яких є передусім комп'ютерні програми та бази даних. Визначено підходи щодо правової охорони прав особистого та майнового характеру для фізичної та юридичної особи. З'ясовано підстави для охорони об'єктів творчої діяльності ІТ-компаній авторським чи патентним правом. Наведено характеристику патентів українських ІТ-компанії, які охороняють, наприклад, ідею цифрового активу [12].

Переконалися, що для правового регулювання відносин щодо цифрових продуктів, які постають об'єктами права інтелектуальної власності ІТ-компаній, виникає потреба звернутися до зобов'язального законодавства, а саме: для розпорядження майновими правами на ІВ виникає потреба у заключенні відповідних договорів. Встановлено особливості першої у світі угоди між українськими компаніями з купівлі-продажу токена блокчейну Bitbon як нематеріального активу [13]. Водночас, усвідомлено, що досягненню цієї мети сприятиме дослідження комплексних правовідносин (цивільно-інформаційних), тобто, правових засобів як права інтелектуальної власності, так і інформаційного права.

Поетапна перевірка висунутої наукової гіпотези дозволила дійти висновку щодо її справедливості. Водночас, задля досягнення поставленої мети пропонуємо формування відповідного механізму – системного утворення, невід'ємними складовими якого є: правова охорона (правові засоби права інтелектуальної власності

й інформаційного права); технологічна охорона (інструменти цифрової економіки). Між зазначеними складовими – зв'язки взаємосприяння. Тобто, існує потреба у комплексному використанні правових та технологічних інструментів охорони права інтелектуальної власності, що вимагає свого подальшого опрацювання.

Отримані у роботі результати свідчать про те, що автор послідовно відстоює ідею суспільства знання [5], у якому охороняються права особи – фізичної та юридичної. Підкреслюється, що впровадженню зазначеної ідеї сприяло також конструктивне використання підходу щодо взаємодії галузей права. Ґрунтовний аналіз суспільних відносин, що виникають під час охорони права ІВ, дозволив дійти висновку стосовно різного характеру цих відносин: інформаційні, майнові, публічно-сервісні, трудові та ін. До того ж, встановлено, що виникають складні суспільні відносини, елементи яких регулюються нормами різних галузей права (зокрема, цивільного, інформаційного, адміністративного права). На нашу думку, необхідні подальші ґрунтовні дослідження правового регулювання складних суспільних відносин, що виникають під час охорони права ІВ в умовах цифрової економіки в Україні, за участі фахівців з різних галузей права.

Список використаної літератури

1. G20 Програма по розвитку и сотрудничеству в сфере цифровой экономики (Итоговый документ 2016). URL: <http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/> (дата звернення: 12.05.2020)
2. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації : Розпорядження Кабінету Міністрів України від 17.01.2018 р. № 67-р. URL: <https://www.kmu.gov.ua/npas/pro-shvalennya-konceptsiyi-rozvitku-cifrovoyi-ekonomiki-ta-suspilstva-ukrayini-na-20182020-roki-ta-zatverdzhennya-planu-zahodiv-shodo-yiyi-realizaciyi> (дата звернення: 15.05.2020)
3. Яновицька Г.Б., Кучер В.О. Цивільне право України: підручник: в 2 т. Т. 1. За ред. Г.Б. Яновицької. Львів: «Новий Світ-2000», 2014. 444 с.

4. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони: ратифікована із заявою Законом № 1678-VII від 16.09.2014 р. URL: https://zakon.rada.gov.ua/laws/show/984_011 (дата звернення: 15.05.2020)

5. Арістова І.В. Наука «Інформаційне право» на новому етапі розвитку інформаційного суспільства. *Правова інформатика*. 2011. № 1. С. 3-11

6. Про Рекомендації парламентських слухань на тему: «Законодавче забезпечення розвитку інформаційного суспільства в Україні»: Постанова Верховної Ради України від 03.07.2017 р. №1565-VII. *Відомості Верховної Ради України*. 2014. №33. Ст.1163

7. Скакун О. Ф. Теорія держави і права (Енциклопедичний курс): підручник. Вид. 2-е, перероб. і доп. Харків: Еспада, 2009. с. 752

8. Кудь О.О., Кучерявенко М.П., Смичок Є.М. Цифрові активи та їх економіко-правове регулювання : монографія. Харків : Право, 2019. 384 с.

9. Что такое блокчейн простыми словами. URL: <https://prostocoin.com/blog/blockchain-guide>(дата звернення: 15.05.2020)

10. Харитонов С.О., Харитонova О.І. IT- право: теорія та практика: навч. посіб. 2-ге вид., доп. Одеса : Фенікс, 2019. 472 с.

11. Арістова І.В., Карпик Ю.А. Вплив цифрової економіки та європейської інтеграції на правотворчість у сфері інтелектуальної власності в умовах розбудови інформаційного суспільства та інформаційного законодавства в Україні. *Modern researches: progress of the legislation of Ukraine and experience of the European Union : Collective monograph*. Riga : Izdevniecība “Baltija Publishing”, 2020. P. 1. P.255-288.

12. Патент на винахід «Спосіб здійснення транзакції з передачі цифрової цінності (цифрового активу) та система передачі цифрових цінностей для його здійснення»: офіційний сайт компанії Simcord. URL: <https://www.simcord.com/ua/legal-information-patents> (дата звернення: 15.05.2020)

13. Система Bitbon: офіційний сайт компанії Simcord. URL: <https://www.simcord.com/ua/bitbon-system> (дата звернення: 15.05.2020)

Тарасюк А.В.

кандидат юридичних наук, головний науковий співробітник Наукової лабораторії забезпечення інформаційної та кібернетичної безпеки НДІ інформатики і права НАПрН України

МОРАЛЬНО-ЕТИЧНІ ЗАСАДИ У КІБЕРБЕЗПЕЦІ ЛЮДИНИ

Людська спільнота на сучасному – інформаційному етапі свого розвитку – це складне багаторівневе соціальне утворення, система, складена з багатьох компонентів, задіяних в інформаційних комунікаціях. Не забуваючи про техніко-логічні характеристики вказаних комунікацій, зазначимо, що під час аналізу інформаційної взаємодії та інформаційного обміну слід неодмінно зважати, що це – взаємини людини й соціальних елементів системи (суспільних структур), котрі виражають інтереси окремих осіб, груп людей, а також великих спільнот. Головним, що вирізняє зазначене високоорганізоване соціальне утворення в інформаційну епоху, є його цілковите підпорядкування засадам результативної інформаційної комунікації.

Варто також, на нашу думку, пам'ятати, що існуючі форми та способи комунікацій здійснюються задля задоволення потреб, реалізації інтересів і цінностей особи й суспільства, а не заради інформаційної взаємодії як такої. Саме це, вважаємо, і є ціннісним самопізнанням під час аналізу інформаційної картини світу. Саме в цьому полягає сутність аксіологічного підходу до вивчення інформаційної сфери – процесів, взаємодії, обміну, продукції, послуг та ін.

Широко застосовуване сьогодні поняття «інформаційне» стосовно сучасного суспільства замінило собою цілу низку термінів на його позначення, як от: постіндустріальне, пост буржуазне (пост капіталістичне), пост ринкове, пост традиційне, пост історичне, технотронне, програмоване, компетентне (засноване на знаннях – «the knowledgeable society») [1], конвенціональне [2] тощо. Поняття «постіндустріальне», на думку Д. Белла, є більш змістовним для

означення суспільства, натомість його характеристика як інформаційного дозволяє надати поняттю точнішого специфічного навантаження. І хоча це «навантаження» учений вважав руйнацією понять, якими зазвичай послуговувалися для аналізу суспільних відносин, у своїх працях він користувався обома термінами – постіндустріальне суспільство й інформаційне суспільство [3].

Своєю чергою, М. Кастельс пропонував користуватися в таких випадках терміном «інформаціональне суспільство». Дослідник уважав, що інформація, інформування в сенсі передавання певного знання завжди відігравали важливу роль, тоді як для відображення певної атрибутивної властивості особливої форми соціальної організації більше підходить термін «інформаціональний». Зазначена властивість полягає в тому, що в теперішній історичний проміжок усі способи трансляції інформації перетворилися на підставі економіки, структурування суспільства та здійснення владних повноважень [4, с. 42].

За такої вельми значної непослідовності концептуальних підходів деякі дослідники визначають інформаційне суспільство як «високу стадію розвитку постіндустріального суспільства» (Е. Масуда), «розвинене індустріальне суспільство (У. Мартін), «електронно-цифрове суспільство» (Д. Тапскотт).

Як бачимо, розвиток інформаційного суспільства має нелінійний характер та іншу специфіку, зокрема:

- взаємозалежність кількості та якості інформації;
- складність розрізнення достовірної та хибної (неправдивої, вигаданої) інформації;
- брак надійних критеріїв перевірки достовірності інформації;
- маніпулятивний вплив хибної інформації на індивідуальну та суспільну свідомість;
- стереотипне сприйняття інформації, хибні, фальшиві інформаційні цінності;
- переривчастість (атомізація) інформаційного середовища, яка зумовлює серйозні ризики у сфері інформаційної безпеки.

Ускладнення інформаційних відносин зумовлює виникнення різноманітних інформаційних посередників, котрі відіграють роль зв'язкових між окремим користувачем з його особистим просто-

ром та інформаційним полем у глобальному інформаційному середовищі. У такому полі інформаційної взаємодії, в якому змушена діяти людина, створюються інформаційні примари (фантоми), інформаційні артефакти та інформаційні сурогати. Спочатку ці інформаційні фантоми співіснують з реальністю, врешті-решт витісняючи останню, залишаючи натомість сурогатну квазіінформаційну завісу. Якщо людина не помічає цього, вона починає керуватися правилами цієї хибної реальності.

Для побудови адекватної безпекової політики практика захисту інформації неодмінно має враховувати морально-етичні аспекти, котрі потребують також подальшого вивчення. Вказані заходи протидії можна вважати універсальними, позаяк вони назагал стосуються усіх рівнів захисту кібернетичної сфери.

Спробу проаналізувати безпеку як соціальне явище, дослідити взаємозв'язок і взаємозумовленість безпеки людини, суспільства й безпеки держави вперше здійснив англійський філософ 17 століття Томас Гоббс. Учений виявив соціальну природу безпеки, залежність її забезпечення від формування у суспільстві відповідних поведінкових норм [5].

Оскільки безпекові питання стосуються усіх сфер життєдіяльності суспільства, їх розв'язання тривалий час покладалося виключно на державу, яка формувала відповідну систему забезпечення безпеки, користуючись своїми владними повноваженнями. Тим часом, ІТ-системи у своїй еволюції набули соціальних якостей, а також стали джерелом підвищеної небезпеки. Людина в цих відносинах стає водночас і об'єктом, і суб'єктом, і первинним джерелом їх виникнення. Людина впливає на інформаційні відносини одночасно як організуючий і як деструктивний чинник.

Розв'язується вказана суперечність шляхом подальшого розвитку, вдосконалення технологій самого сучасного соціуму, які унеможливлюють похибки в його інформаційно-технологічній діяльності. Утім, позаяк людина є постійним носієм загроз, досягти рівня цілковитого гарантування інформаційної (кібернетичної) безпеки не уявляється можливим.

Як доводилося раніше, захистом від шкідливих впливів, зокрема інформаційних, є моральні чинники й інтелектуальні властиво-

сті, ціннісні настанови, себто підвищення інтелектуального рівня суспільства виступає сьогодні важливим захисним механізмом. І це попри те, що для захисту від надмірних обсягів інформації, передовсім негативної й низької якості, в теперішній час застосовуються спеціальні технічні засоби, зокрема різноманітні пошукові програми чи формалізатори інформаційних ресурсів, пізнавальні стратегії звернення до інформації тощо. Утім, вказані стратегії здатні реально звільнити людини, на котру обрушилися величезні інформаційні потоки, лише в тому разі коли сама людина спроможна адекватно їх оцінити. Розв'язуючи проблеми інформаційної сфери, у тому числі свободи взаємодії користувачів, не слід забувати, що людина має навчитися сприймати й усвідомлювати знаки, позаяк насамперед когнітивним вимогам підпорядковуються доступ до інформації та автономність суб'єкта пізнання.

Сучасна суспільна практика потребує від людини вдосконалювати свої знання та вміння, оскільки від цього вирішальною мірою залежить її здатність сприймати (споживати), переробляти, зберігати, передавати, а також виробляти інформацію. Сьогодні якість діяльності людини й суспільства, рівень розвитку пізнавальних і творчих потенцій людини, які проявляються в методах організації життєдіяльності й осягнення світу, багато в чому залежить від інформаційної культури. Тому остання набуває для кожної людини й соціуму загалом життєво важливого значення.

На зайвим убачається підкреслити ще раз, що, ґрунтуючись лише на адміністративних, фізичних і технічних засобах, ефективну систему кібер захисту сформувати неможливо, оскільки її дієвість залежить передовсім від людини, її професійних та особистісних якостей. Її стійкість зумовлюється професіоналізмом і згуртованістю колективу, а підвищення результативності відбувається за рахунок законодавчих і морально-етичних заходів. Утім, звісно, найдосконаліші правові акти й найефективніша кадрова політика не є гарантією належного розв'язання безпекових проблем.

Головним чинником формування системи кібер захисту інформації й регулятора людської діяльності в інформаційній сфері у процесі забезпечення кібербезпеки як соціального феномену є морально-етичні принципи, відповідальність кожного суб'єкта, які

базуються на загальноприйнятих правилах поведінки в суспільстві й підкріплюються законодавчими заходами. Можна також зазначити, що в теперішній час відчувається нагальна потреба цілеспрямованого формування інформаційної культури суспільства, від чого значною мірою залежить успішне розв'язання проблем кібербезпеки й подолання викликів, котрі виникають у процесі творення світового інформаційного простору.

Література:

1. Lane R.E. The Decline of Politics and Ideology in a Knowledgeable Society American Sociological Review Vol. 31, No. 5 (Oct., 1966), pp. 649-662
2. Pakulski J., Waters M. The Death of Class. First Published July 1, 1997 Volume: 21 issue: 2, page(s): 192-193
3. Белл Д. Грядущее постиндустриальное общество. М.: Academia, 2004. 944 с.
4. Кастельс М. Информационная эпоха : экономика, общество и культура. Изд. дом ГУ-ВШЭ, 2000. 608 с.
5. Гоббс Т. Сочинения в 2 Т.: М.: Мысль, Т. 2. 1991. 731 с.

Білоус О.А.

викладач Ірпінського державного
коледжу економіки та права

ЗАПОБІГАННЯ КОРУПЦІЇ У ПРЕДСТАВНИЦЬКИХ ОРГАНАХ ВЛАДИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

На сьогоднішній день корупція залишається одним з негативних соціальних явищ, що турбує українське суспільство і державу. Вимога боротьби з корупцією була однією з рушійних сил Революції Гідності і є одним з пріоритетів, що не втрачає свого значення і до цього часу. Зауважимо, що в умовах цифрових трансформацій удосконалюється нормативно-правова база запобігання корупції. Зокрема, прийнято антикорупційну стратегію «Засади державної антикорупційної політики в Україні», яка передбачає посилення відповідальності органів державної влади та посадових осіб в реалізації державної антикорупційної політики. Україна здійснила перші кроки до антикорупційних реформ, які спрямовані на запобігання, виявлення та покарання корупціонерів.

Для розробки антикорупційної політики в представницьких органах влади були проаналізовані рекомендації міжнародних організацій, включаючи посилення правового, інституційного, фінансового і кадрового зміцнення антикорупційних структур, міжнародного співробітництва та покращення взаємодії з міжнародними організаціями з метою більш ефективної боротьби з корупцією. За результатами першого, другого і третього раундів оцінювання Групи держав проти корупції (GRECO) Україна не має невиконаних рекомендацій. Водночас, довготривале існування корупції в представницьких органах влади не дає можливості швидкого її подолання.

Визначальним нормативно-правовим актом у сфері антикорупційної політики України є Антикорупційна стратегія на 2018-2020 роки, на основі якої здійснюється реалізація передбачених в ній заходів [1, с. 2].

Соціологічні опитування свідчать, що в Україні існує високий рівень недовіри до представницьких органів влади. За цих умов потрібно налагодити взаємодію органів державної влади з інститута-

ми громадянського суспільства.

Під впливом міжнародних організацій в Україні створено систему органів державної влади, головним завданням яких було подолання корупції в представницьких органах влади, зокрема, Національне антикорупційне бюро України (Далі - НАБУ), Національна агенція запобігання корупції (Далі - НАЗК), Національне агентство України з питань виявлення, розшуку та управління активами, одержаними від корупційних та інших злочинів (Далі - АРМА), Спеціалізована антикорупційна прокуратура. Відзначимо, що вони розпочали свою роботу в дуже важких умовах.

На нашу думку, для того, щоб подолати корупцію в представницьких органах влади потрібно впровадити стійкі правила доброчесності, дотримання правил справедливих і прозорих виборів, рівня демократичної політичної системи.

Оприлюднені результати електронного декларування доходів засвідчили непоодинокі випадки володіння народними депутатами України майном та коштами, що не відповідають їх доходам та порушує стандарти доброчесності. При цьому депутатська недоторканність ускладнює механізм притягнення таких осіб до кримінальної відповідальності.

Рекомендації GRECO надали рекомендації про необхідність запобігання корупції у представницьких органах влади та органах місцевого самоврядування. Верховній Раді України було запропоновано із дотриманням відповідного рівня прозорості опрацювати законопроекти щодо прийняття правил проведення скороченої законодавчої процедури у Парламенті та гарантії того, що вона використовується лише в окремих випадках. Що стосується вжиття подальших необхідних заходів для припинення уникнення обмежень на зайняття народними депутатами України підприємницькою діяльністю не тільки на законодавчому рівні, а й на практиці, то потрібно ще раз переглянути законодавчу базу, щодо даної проблеми [1, с. 38].

На жаль, норми Закону України «Про вибори народних депутатів України» та Закону України «Про вибори депутатів місцевих рад та сільських, селищних, міських голів» залишають можливості для корупційних зловживань при формуванні партійних списків та для технологій підкупу виборців під час виборів. Тому GRECO

та Венеціанська комісія підтримують перехід України до нової виборчої системи, заснованої на відкритих списках і багатомандатних виборчих округах [1, с. 231].

Законодавство про вибори народних депутатів України, Президента України та про політичні партії регламентує права та обов'язки розпорядників виборчого фонду, порядок формування виборчого фонду та використання його коштів та звітності про надходження та використання коштів виборчого фонду, обмеження у здійсненні внесків на підтримку політичних партій тощо. Також в ньому визначено компетенцію органів державної влади, які здійснюють контроль за дотриманням вказаних норм та встановлено відповідальність за порушення порядку фінансування політичної партії, передвиборної агітації, агітації з всеукраїнського або місцевого референдуму. Однак, зі 344 зареєстрованих залишається близько 100 політичних партій, які відсутні за місцезнаходженням або не бажають подавати звіти до НАЗК. Наразі у НАЗК немає необхідного нормативного інструменту примусу політичних партій до виконання ними обов'язку публічного звітування про свої фінанси та дотримання встановленого порядку отримання внесків від фізичних та юридичних осіб. Сьогодні існує велика проблема щодо доопрацювання цих законів.

В Україні не повністю завершено формування законодавчої та інституційної основи для вироблення та реалізації антикорупційної політики, допущено виникнення колізій між відповідними законодавчими актами в частині повноважень органів по боротьбі з корупцією та забезпечення їх належної співпраці, та не вжито заходів для їх оперативного усунення. Потрібно подальше приведення вітчизняного законодавства у відповідність до міжнародних договорів України (Конвенцією ООН проти корупції, Цивільною конвенцією про боротьбу з корупцією, Кримінальною конвенцією про боротьбу з корупцією) та практики їх застосування, також забезпечити залучення широкого кола представників громадянського суспільства до процесів боротьби з корупцією на всіх рівнях.

Проблема полягає і в тому, що у видатках державного бюджету не передбачено кошти на діяльність НАЗК для залучення ним вітчизняних і зарубіжних аналітичних центрів, фахівців і незалеж-

них експертів із формування державної антикорупційної політики та оцінки її результатів [2, с. 17].

В законодавстві України бракує визначення понять лобістської діяльності, не визначено кола суб'єктів такої діяльності, їх прав та обов'язків, ведення реєстру лобістів та лобістських контактів тощо. Саме відсутність законодавчого врегулювання лобіювання обмежує можливості запобігання корупції у Верховній Раді України і органах виконавчої влади та місцевого самоврядування. Розробка та ухвалення закону про правові засади лобіювання із застосуванням кращого міжнародного досвіду та із врахуванням національної специфіки процедур правотворчості, є вкрай актуальними.

Значним кроком у вдосконаленні нормативно-правової бази України у сфері запобігання корупції є прийняття 6 грудня 2019 р. Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення». У ньому, зокрема, забезпечення міжнародного співробітництва у сфері запобігання корупції покладається на:

- Міністерство юстиції України - щодо виконання судових рішень, які стосуються конфіскації доходів, одержаних злочинним шляхом;
- Генеральну прокуратуру України, Національне антикорупційне бюро України - щодо вчинення процесуальних дій у межах кримінального провадження щодо легалізації (відмивання) доходів, одержаних злочинним шляхом;
- Службу безпеки України та Міністерство закордонних справ України

При поданні пропозицій до комітетів Ради Безпеки ООН стосовно включення фізичних, юридичних осіб та організацій до відповідних санкційних переліків Служба безпеки України та Міністерство закордонних справ України повинні:

- додержуватися визначених відповідними комітетами Ради Безпеки ООН процедур та стандартних форм внесення осіб до відповідних переліків;
- надавати повну, наскільки це можливо, інформацію щодо запропонованої до включення особи чи організації, а саме інфор-

мацію, достатню для ідентифікації фізичних осіб, організацій та юридичних осіб, та, за можливості, інформацію, необхідну Міжнародній організації кримінальної поліції - Інтерполу для видачі спеціального повідомлення;

- детально, наскільки це можливо, викладати фактичні обставини справи та обґрунтування щодо включення до переліку та надавати таку інформацію на запит, крім інформації з обмеженим доступом, яка не може бути надана до відповідного комітету;

- зазначати, чи може оприлюднюватися відповідними комітетами статус України як країни, яка подала пропозиції про включення до відповідних санкційних переліків.

Контроль за виконанням законів у сфері запобігання та протидії здійснюється органами державної влади в межах їх повноважень та в порядку, визначеному Конституцією та законами України [3, ст. 36].

Спеціально уповноважений орган щороку до 31 березня року, наступного за звітним, подає до Верховної Ради України за встановленою формою звіт про стан запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом .

Сформулюємо основні напрямки трансформації нормативно-правової бази щодо запобігання корупції у представницьких органах влади в умовах цифрових трансформацій:

- удосконалення інституту проведення антикорупційної експертизи чинних нормативно-правових актів та проектів нормативно-правових актів, а також рішень регуляторного характеру і їх проектів, шляхом внесення до законодавства відповідних положень, у тому числі щодо необхідності врахування висновків антикорупційної експертизи або обґрунтованого їх відхилення;

- забезпечення об'єктивного розгляду в органах державної влади і місцевого самоврядування всіх висновків незалежної антикорупційної експертизи, що надійшли до них;

- запровадження широкого інформування громадськості про розроблені законопроекти, їх мету та прогноз результатів;

- посилення фінансової дисципліни політичних партій та забезпечення виконання політичними партіями виконання їхнього обов'язку публічно звітувати про майно, доходи, витрати і зобов'яз-

зання фінансового характеру, дотримуватись встановленого порядку отримання внесків від фізичних та юридичних осіб;

- запровадження електронного декларування звітності політичної партії;

- налагодження системного діалогу між громадянським суспільством і представницькими органами влади;

- вжиття заходів з метою підвищення обізнаності щодо питань доброчесності у Верховній Раді України та в органах місцевого самоврядування як на індивідуальному рівні (надання консультацій), так і на інституційному рівні (навчання, інституційні дискусії з етичних питань тощо) [4, ст. 11].

Виходячи з того, що основними завданнями представницьких органів влади є забезпечення виконання нормативно-правових актів України та забезпечення прав і свобод громадян на відповідній території, неабияка увага повинна приділяти заходам протидії корупції, яка зумовлює деструктивний вплив на суспільний розвиток.

Список використаної літератури:

1. Державна антикорупційна політика і запобігання та протидія корупції на публічній службі в органах державної влади і органах місцевого самоврядування : монографія / авт. кол. : В. В. Василевич, Т. Е. Василевська, А. В. Савченко, В. Л. Федоренко (кер. авт. кол.) та ін. ; за ред. Ю. В. Ковбасюка, В. Л. Федоренка. – К. : Ліра-К, НАДУ, 2016. – 524 с.

2. Соснін О.О. Про необхідність запобігання використанню світового досвіду в боротьбі з корупцією у вітчизняній практиці / О.О.Соснін // Віче. – 2014. - №1- С.17

3. Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення: Закон України від 06.12.19 № 361-IX. *Відомості Верховної Ради. Голос України*. 2019. №251 ст.36

4. Про запобігання корупції: Закон України від 14 жовтня 2014 №1700-VII. *Відомості Верховної Ради*. 2014. №49. ст. 11

Єсімов С.С.

кандидат юридичних наук, доцент,
доцент кафедри адміністративно-правових дисциплін Львівського державного університету внутрішніх справ

СУЇЦИДАЛЬНА ПОВЕДІНКА ТА ІНТЕРНЕТ

Формування правової держави, яка охороняє правовий статус особи, створює надійні механізми захисту правового статусу, неможливо без затвердження в соціальній свідомості неухильного дотримання прав кожної особи, оскільки всі права людини ґрунтуються на природному та невід'ємному праві – праві на життя. Право на життя офіційно закріплено в Загальній декларації прав і свобод людини. Кожна людина має право на життя, на свободу, на особисту недоторканність [1]. Ці цінності проголошує Конституція України [2]. Дане право є безпосередньо діючим. Це ставить обов'язок держави в особі її органів захищати це право.

Захист права на життя здійснює кримінальне законодавство України, за допомогою норм, які охороняють життя особи. Кримінальний кодекс України встановлює відповідальність за вбивство; доведення особи до самогубства або до замаху на самогубство, що є наслідком жорстокого з нею поводження, шантажу, систематичного приниження її людської гідності або систематичного протиправного примусу до дій, що суперечать її волі, схилення до самогубства, інших дій, що сприяють вчиненню самогубства [3].

Захист права особи на життя здійснюється різними матеріальними та процесуальними галузями права. Захист права на життя відображено в охоронних нормах Кримінально-процесуального кодексу України; Кодексу України про адміністративні правопорушення, Кримінально-виконавчого кодексу України та інших нормативно-правових актів.

В Україні проблема захищеності життя особи залишається декларативною. У сфері охорони особи відсутня концептуально закріплена кримінально-правова політика. КК України не вказує на

особливу природу охорони права особи на життя в якості пріоритетного завдання.

Виділення людського життя особливим чином в нормах Загальної частини КК України необхідно, з огляду на те, що життя людини, виступаючи об'єктом злочинного зазіхання, характеризується рядом виняткових ознак: унікальність кожної людської особистості; безцінність людської особистості та неможливість порівняння; незворотність позбавлення життя особи; винятковість наслідків (при боротьбі кримінально-правовими заходами відбувається запобігання наслідків, що настали, але не усунення причини посягання).

Проблемою є суїцидальна поведінка особи. Суїциди скоюють люди, маючи на різні причини, тому для психології, кримінології, права важливо систематично проводити аналіз чинників, що викликали бажання осіб на суїцид, з метою попередження такої поведінки.

Всесвітня організація охорони здоров'я зазначає, що суїцид стає третім чинником смерті людей у віці від 15 до 24 років.

Суїцид це складний феномен, що складається з біологічних, соціальних, психологічних, культурних і філософських аспектів. Кримінологи говорять, що злочини, передбачені ст. 120 КК України, носять латентний характер.

Загальні чинники суїцидів визначити неможливо, через велику кількість факторів. Головну роль відіграють зовнішні фактори, але є й внутрішня психологічна установка особи, яка формується суспільством і особою. Рівень смертності від самогубств залежить від: внутрішньої самосвідомості особи; генетичних факторів; загальної економічної депресивності регіону, де проживає особа; етнокультури регіону; депресії, психологічних розладів.

Якщо брати до уваги найбільш вразливу в психологічному аспекті групу людей – неповнолітніх, чинниками виступають: кризові відносини з батьками; психологічні перевантаження у навчанні; невдалий досвід першого кохання; некомпетентність педагогів, які здійснюють виховання в закладі освіти; відсутність обачності та чуйності батьків, щоб у дитини не виникли думки про самогубство.

Праву на життя, протиставляється право на смерть. Незважаючи на невизначеність у науковому аспекті зазначеного права, на нашу думку, воно може існувати тільки тоді, коли бажання піти з

життя не було сформовано зовнішніми факторами, шляхом умисного створення іншими особами таких ситуацій, які провокували вчинення суїциду.

З розвитком мережі Інтернет з'явилися зовсім нові способи психологічного впливу на особу з метою викликати психічний розлад, який в науці визначений як кібер булінг (розуміється як цькування в мережі), крайня форма кібер булінгу - кібер боулінг суїцид (від англ. cyberbullycide) внаслідок зіткнення з прямою або непрямою агресією он-лайн. Визначення булінгу дано в законі України від 18 грудня 2018 року № 2657-VIII «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» [4].

Кібербуліцид є небезпечний вид агресії з огляду на те, що зловмисники використовують невпевненість і вразливість жертви в певний період життя з метою заподіяння психологічної травми та приниження, доводять до самогубства. Дії реалізуються в формі створення Інтернет-спільнот, діяльність яких спрямована на доведення особи до самогубства (як головна мета, на відміну від кібербулінгу).

Законодавством встановлена кримінальна відповідальність за доведення до самогубства або до замаху на самогубство, що є наслідком жорстокого поводження, шантажу, систематичного приниження людської гідності або систематичного протиправного примусу до дій, що суперечать волі, схиляння до самогубства, інших дій, що сприяють вчиненню самогубства. Це реалізація боротьби тільки з наслідками явищ, які лежать в основі таких діянь, але не з самими чинниками.

З огляду на підвищену віктимність серед неповнолітніх, велику роль грає педагогічна та соціально-психологічна робота з неповнолітніми.

До підлітка, який обговорює ідею суїциду або намагається це здійснити, необхідна пильна увага педагогів і соціальних психологів, які в обов'язковому порядку повинні бути у закладі освіти. Соціальний психолог зможе ефективним способом вести моніторинг неповнолітніх, які потрапили в складну життєву ситуацію.

Профілактика суїциду педагогами та психологами в закладах освіти може здійснюватися за напрямками: виявлення та моніторинг

неповнолітніх, емоційне благополуччя яких викликає у соціального педагога сумніви; зняття психологічної напруги в психотравмуючій ситуації; вироблення компенсаторних механізмів поведінки; формування адекватного ставлення до життя. Для реалізації на пряму доцільним і ефективним буде створення програмно-методичного забезпечення психопрофілактичних заходів, спрямованих на виявлення передумов ризику суїциду у неповнолітніх.

Доцільно зауважити, що закон «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» передбачав реалізацію зазначених заходів, але окрім вказівок Національної поліції щодо проведення превентивних заходів загальної профілактики (виступи офіцерів ювенальної поліції у закладах освіти та проведення оперативно-розшукових заходів за фактами наданими засобами масової інформації підрозділами кіберполіції), зазначені заходи не надійшли у територіальні органи поліції. Ці заходи вимагають нормативного закріплення і організації функціонування кваліфікованої психолого-педагогічної допомоги у закладах освіти, спеціалізації офіцерів ювенальної поліції.

Одним з елементів протидії кібер суїциду повинна бути психолого-педагогічна робота з батьками неповнолітніх, які перебувають в зоні ризику кібербулліцида. Адже налагоджені сімейні відносини між неповнолітніми та батьками, виховання в теплій атмосфері прийняття світоглядних установок, буде протидіяти таким злочинам.

Досить ефективним у протидії мережному суїциду буде створення спеціалізованих Інтернет-спільнот при органах освіти, де кожна людина могла розповісти про підозрілі записи на сторінках різних форумів і повідомляти інформацію не модераторам сайтів, а спеціальним співтовариствам, створеним для цих цілей. Варто створити сайти допомоги потенційним жертвам.

Досвід Ізраїлю, Німеччини, Швеції, які успішно борються з кібер булінгом, що приводить до суїциду, показує, що допомога особам і негайне повідомлення адміністраторами сайтів поліції про звернення особи за допомогою, показує, що допомога ефективніша в боротьбі з мережевим суїцидом, ніж методи блокування сайтів.

Вирішення проблеми з Інтернет суїцидом доцільно починати зі стабілізації психологічного стану особи, за допомогою надання

стабільної і ефективної психологічної допомоги, оскільки причини суїциду численні.

Важливу роль у межах протидії таким злочинам грає кримінально-правове регулювання, хоч це здійснюється побічно протидіючи наслідкам, а не чинникам. Але за допомогою КК України держава реагує на суспільно-небезпечні діяння, реалізуючи положення ч. 2 ст. 50 КК.

Доведення до самогубства є одним з складних видів злочину, зважаючи на наявність зв'язку між діями суб'єкта та наслідками. Ці злочини мають високий рівень латентності та складно доказові при використанні інформаційно-комунікаційних технологій. У межах кваліфікації злочинів за ч. 3 ст. 120 КК України можуть викликати проблеми у осіб, які застосовують право, такі елементи, як наявність систематичного приниження людської гідності в мережі Інтернет. Для доведення до самогубства дії винного необов'язково можуть носити систематичний характер.

Доцільно виключити з ч. 1 ст. 120 КК України ознаку систематичності. Склад злочину, передбачений ст. 120 КК України, за конструкцією об'єктивної сторони є матеріальним. Це означає, що обов'язковому доведенню особою, яка застосовує право, підлягає причинний зв'язок між фактом самогубства або замахом і протиправними діями винного. За цим критерієм буде складно відрізнити наявність суїциду викликаного діями суб'єкта у соціальній мережі. Але це можливо, оскільки вчені відносять до способу скоєння вбивства – гіпноз, тобто заподіяння смерті не шляхом доведення особи до самогубства, а шляхом умисного заподіяння смерті, але руками потерпілого.

З метою охорони права на життя, доцільно посилити кримінальну відповідальність за діяння, передбачене ч. 3 ст. 120 КК України, оскільки, з огляду на особливий об'єкт кримінально-правової охорони, це найбільш повно сприятиме положенням, передбаченим ст. 1 та ч. 2 ст. 50 КК України.

Доцільно відзначити, що в боротьбі з суїцидом в Інтернеті не можна покладатися тільки на законодавче закріплення прав і гарантій особи, необхідно комплексно та максимально ефективно підходити до вирішення кримінологічно-небезпечної та деструктивної для суспільства проблеми, як мережевий суїцид.

Необхідно враховувати: формування на державному рівні установ і Інтернет-спільнот, які будуть на постійній основі здійснювати виявлення, припинення та поширення мережевого суїциду; комплексний психолого-педагогічний підхід щодо неповнолітніх; постійну профілактику суїциду в частині надання кваліфікованої психологічної допомоги; формування у кожній особі (у неповнолітніх, зокрема) навички цифрової компетенції, яка би дозволяла кожній людині використовувати інформаційно-комунікаційні мережі на благо собі та суспільству, мінаючи всі негативні наслідки Інтернет-простору.

Право на життя – одне з головних прав людини є невідчужуваним, не передається, повинно охоронятися та захищатися державою. Тільки комплексний підхід до вирішення проблеми злочинного посягання на життя зможе в повній мірі реалізовувати положення Конституції України.

Список використаної літератури

1. Загальна декларація прав людини. Законодавство України. URL. https://zakon.rada.gov.ua/laws/show/995_015
2. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР / Відомості Верховної Ради України. 1996. № 30. Ст. 141.
3. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III / Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.
4. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) : Закон України від 18.12.2018 р. № 2657-VIII / Відомості Верховної Ради України. 2019. № 5. Ст. 33.

Конотопенко О.П.

кандидат філософських наук,
доцент кафедри правових наук та
філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського

Лапшин С.А.

кандидат історичних наук,
доцент кафедри правових наук та
філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського

**ПУБЛІЧНА ІНФОРМАЦІЯ І ВІДКРИТІ ДАНІ ЯК ЗАСІБ
ЗАБЕЗПЕЧЕННЯ ПРАВ І БЕЗПЕКИ ГРОМАДЯН В УМОВАХ
ЦИФРОВИХ ТРАНСФОРМАЦІЙ**

В умовах розвитку інформаційного суспільства власне інформація є не просто економічним, політичним і соціальним ресурсом, а й тим чинником, який у сфері діяльності органів державної влади здатний ефективно вплинути на корупційну ситуацію в державі. Доступ до публічної інформації може сприяти відкритому та прозорому обговоренню всіх існуючих проблем через діалог між владою та громадянським суспільством.

Зазначена проблематика актуалізується недовірою громадян до органів державної влади і необхідності переходу від закритості всіх гілок влади до відкритості, гласності та прозорості їх діяльності. Тому дослідження публічної інформації мають особливу значущість, тим більше, якщо ця проблема пов'язана з правами людини, які на сучасному етапі державотворення України не лише займають привілейоване становище у формуванні правової, соціальної держави та громадянського суспільства, а й визначаються як чинник стратегії сталого розвитку держави та суспільства.

На сьогодні та в перспективі питання доступу до публічної інформації матиме переважно глобальний характер. Ця обставина підвищує вагомість вказаної проблематики та вказує на її як теоретичне, так і практичне значення.

Публічна інформація – це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим законом. Публічна інформація є відкритою, крім випадків, встановлених законом [1].

Вся інформація, що є в органах державної влади та органів місцевого самоврядування є публічною інформацією. Умови використання публічної інформації визначаються Законом України «Про доступ до публічної інформації», який покликаний сприяти відкритій діяльності органів влади, їх підзвітності суспільству. Саме цей закон дав можливість фізичним та юридичним особам отримувати інформацію за запитом у термін не більше п'яти робочих днів. Він зобов'язав розпорядників інформації не лише надавати повну, актуальну інформацію у відповідь на запит, а й оприлюднювати її у визначені законом строки.

Сьогодні в Україні у сфері відкритих даних відбувається активний процес створення стандартів, зокрема того, які формати даних треба використовувати, як з ними працювати, як захищати тощо. Ресурси державних порталів (*.gov.ua) стали зачинателями у цій галузі. Здійснюючи перші кроки на довгому шляху до відкритого суспільства, вони визначають основний напрям розвитку українського ринку відкритих даних. За останні роки відкриті дані продукують економічні інновації, соціальні зміни, нові форми політичної і державної звітності.

Відповідно до концепції кривої розвитку, ринок проходить у процесі росту п'ять основних етапів: 1) формування; 2) зростання; 3) насичення; 4) поступове зниження оборотів; 5) згасання ринку. Але це лише одна із теорій. Перспективи ринку відкритих даних в Україні можуть не лише її змінити, а й дати нові стандарти взаємодії влади і громадськості.

Важливо хоча б мимохідь згадати основні сектори ринку відкритих даних. Головними в оцінці ринку є розуміння його кордонів, де він починається та закінчується (умовно чи фактично).

Наразі можна виокремити п'ять рушійних сил:

1. Офіційні державні портали, реєстри та системи. Актуальним для цих ресурсів є питання якості даних. На деяких порталах дані можуть розміщувати у вигляді сканкопій, у форматах pdf, gif, jpg. Часто замість реальних наборів даних викладають сміттєві файли.

2. Електронні сервіси на базі відкритих даних. Ідеться про ресурси, які використовують різні джерела інформації, міксують дані і видають якісно нову інформацію. Цей сегмент також тільки розвивається.

3. Ресурси відкритих даних, які формуються приватним бізнесом, політичними силами, громадськими ініціативами чи приватними особами.

4. Інформаційно-аналітичні ресурси, ЗМІ, які намагаються створити контент, візуалізувати чи надати форму відкритим або умовно доступним даним.

5. Кіберзлодії як обов'язкова частина будь-якої системи, де є чиїсь інтереси, важлива інформація чи гроші.

Ринок відкритих даних допомагає створити нову інфраструктуру на глобальному, національному та локальному рівнях. Сучасне суспільство гостро потребує відповідних умов для їхнього розвитку. Надійна та стабільна взаємодія даних допомагає ухвалювати правильні рішення, надає нам нові послуги та стимулює інновації.

Дані – це факти, за допомогою яких можна перевірити теорію, зрозуміти аномалії та причини, які до цього призвели. Також вони:

- допомагають вибрати альтернативи;
- стимулюють діалог;
- уточнюють прогнози; збільшують поінформованість та обізнаність;
- будують довіру;
- залучають уряд до роботи з громадськістю.

Ринок відкритих даних в Україні функціонує. Спочатку держава відкриває дані. Далі громадськість запускає сервіси, щоб зробити дані корисними. Наступний етап – вироблення культури користування відкритими даними, створення соціального ефекту для ухвалення рішень. І тут до роботи долучаються медіа, аналітики, громадськість.

Використання відкритих даних дає нам цікаву перспективу розвитку: від затребуваності нових професій до створення нових бізнес-моделей. Уже сьогодні дані не можуть існувати самі по собі, їх потрібно перетворювати на інформацію для споживання. Збір і обробка даних має велике значення для тих хто займається створенням електронних сервісів, замовляє аналітику, здійснює розслідування, ухвалює рішення. Обсяг даних важко обробляти без спеціальних навичок і знань. Тому від нас залежить, як швидко ми оволодіємо інформаційно-технічним процесом змін, ґрунтуючись на відкритих даних.

Відкриті дані виступають формою, в якій оприлюднюється публічна інформація. Важливими характеристиками відкритих даних є вільне та безоплатне поширення – будь-хто може їх вільно копіювати, публікувати, поширювати, використовувати. Також вони мають бути адаптовані до автоматизованого оброблення електронними засобами.

Однак закон не має конкретних вимог щодо форматів, у яких представлені відкриті дані. Тому чимало даних, які нині розміщені на офіційних державних порталах, опубліковані в текстовому (txt, rtf, pdf...), графічному (gif, tiff, jpg...), архівному (zip, 7z...) чи в інших форматах.

Публічна інформація у формі відкритих даних дозволяє її автоматичну обробку електронними засобами, вільний та безоплатний доступ до неї, а також її подальше використання. Розпорядники інформації зобов'язані надавати публічну інформацію у формі відкритих даних за запитом, оприлюднювати і регулярно оновлювати її на єдиному державному веб-порталі відкритих даних та на своїх веб-сайтах. Перелік наборів даних, що підлягають оприлюдненню у відкритій формі, вимоги до формату і структури таких наборів, періодичність їхнього оновлення визначаються Кабінетом Міністрів України.

Можна визначити декілька основних ознаки публічної інформації:

1. Належність інформації до сфери відання та компетенції суб'єкта владних повноважень.
2. Існування інформації в певній матеріалізованій формі.
3. Знаходження інформації та її носіїв у володінні суб'єкту владних повноважень або іншого розпорядника публічної інформації.

Так, до публічної інформації відноситься інформація, отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків. Тобто інформація повинна належати до сфери компетенції конкретного суб'єкту владних повноважень або стосуватися виконання цим суб'єктом своїх обов'язків.

Інформація може бути як отримана від інших суб'єктів інформаційних відносин, так і створена безпосередньо самим суб'єктом владних повноважень. Важливим є застереження, щодо визначеності законодавством компетенції та обов'язків, порядку отримання або створення такої інформації.

В цьому аспекті слід зазначити, що не вся інформація, яка отримується або створюється суб'єктом владних повноважень, його посадовими особами або співробітниками входить до категорії публічна інформація. Так, не може розглядатися як публічна інформація особиста кореспонденція та особисті повідомлення засобів телекомунікації (телефонні дзвінки, електронна пошта), отримані співробітниками суб'єктів владних повноважень.

Матеріалізована форма означає те, що до публічної інформації відноситься лише інформація «відображена та задокументована будь-якими засобами та на будь-яких носіях». Таким чином, законодавство встановлює вимоги щодо матеріалізованої форми представлення публічної інформації у вигляді документу, що виокремлює її від загального поняття інформації. Тобто, для того щоб стати предметом правовідносин, взагалі, відомості або данні повинні мати лише можливість для представлення у формі матеріальних або електронних носіїв інформації, в той же час статус публічної інформації такі відомості або данні можуть отримати лише після перетворення у встановлену законодавством матеріальну форму.

Таким чином лише поєднання таких критеріїв, як належна компетенція, розпорядження інформацією та її відповідне оформлення обумовлює можливість виникнення щодо інформації правовідносин, що врегульовані законодавством про доступ до публічної інформації. Разом з тим особливості правовідносин що виникають з приводу публічної інформації обумовлюються не лише її формальними характеристиками, але й суспільною цінністю та значенням такої інформації. Взагалі, основним суспільним призначенням

будь-якої інформації є задоволення інформаційних потреб суб'єктів інформаційних відносин. На цю властивість інформації, вказував ще основоположник теорії інформації К.Шеннон. Він, в своїй праці «Роботи з теорії інформатики та кібернетики» розглядав інформацію, як кількісний чинник, що змінює початкову (апріорну) невизначеність знань або вибору [2]. Не дивлячись на орієнтацію роботи на науково-технічні аспекти інформації, К.Шеннон вказав і на один з ключових соціальних аспектів інформації – усунення невизначеності для здійснення певного вибору. Іншими словами, отримання належної кількості інформації допомагає окремій особі, групі осіб, або всьому суспільству робити обґрунтований вибір певної поведінки. Зокрема, можливість робити обґрунтований вибір на думку дослідників, найбільшою мірою відображає сутність і мету забезпечення права людини і громадянина на доступ до інформації [3, 99].

Підсумовуючи вищевикладене, можна зробити ряд висновків. По-перше, законодавство передбачає три основні критерії віднесення інформації до категорії «публічна інформація», до яких належать: належність до сфери відання суб'єкта владних повноважень, матеріалізована форма представлення та володіння такою інформацією суб'єктом владних повноважень. По-друге, доступ до публічної інформації забезпечує захист як приватних, так і публічних інтересів. Приватні інтереси стосуються вирішення конкретних справ із суб'єктом владних повноважень, публічні – у забезпеченні громадського контролю за діяльністю суб'єктів владних повноважень та політичного процесу в цілому. По-третє, доступ до публічної інформації реалізується через дві незалежні комунікаційні моделі – модель мовлення, в якій ініціатором виступає розпорядник інформації, та консультаційну модель, в якій ініціатором виступає запитувач інформації.

Список використаної літератури:

1. Закон України «Про доступ до публічної інформації» від 13 січня 2011 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – Ст. 314.

2. Шеннон К. Работы по теории информатики и кибернетике / Клод Шеннон; пер. с англ. – М. : Иностранная литература, 1963 – С. 718.

3. Правове забезпечення інформаційної діяльності в Україні: монографія / за ред. Ю. С. Шемшученка, І. С. Чижа – К. : Юридична думка, 2006. – 384 с.

Гиляка О.С.

кандидат юридичних наук,
начальник управління планування
та координації правових досліджень
в Україні Національної академії
правових наук України

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ОКРЕМИХ ПРАВ ЛЮДИНИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

Використання цифрових технологій породило процеси революційних перетворень в сучасному суспільстві – так звану цифрову революцію, цифрову трансформацію суспільних відносин, яка виражається в застосуванні сучасних цифрових технологій в різних сферах діяльності людини і як фактор динамічного розвитку привела до створення цифрової економіки, формування інститутів цифрового права, нової конфігурації соціальних відносин на базі використання соціальних мереж, Інтернету, інших інформаційно-комунікаційних технологій.

Сучасні цифрові технології формують новий спосіб виробництва, створюють передумови для переходу до нової суспільно-економічної формації, до цифровізації суспільних відносин і самого права, що регулює ці відносини. Цифрова трансформація здійснює безпосередній вплив на реалізацію фундаментальних прав людини, сприяє появі нових прав людини і громадянина як учасника всесвітнього інформаційного, цифрового простору. Плоди цифровізації вимагають осмислення і адекватного формулювання правового механізму регулювання, реалізації та захисту вже існуючих та тих, що тільки формуються прав людини з метою сталого соціально-економічного розвитку, забезпечення реалізації конституційних прав і свобод людини і громадянина.

Технологічні платформи на принципах розподіленого реєстру (blockchain та ін.), Інтернет речей (Internet of Things), штучний інтелект і машинне навчання (artificial intelligence), хмарні сервіси і обчислення (cloud computing), «розумні» комплекси та пристрої (Smart Everything), аналітичні бази великих даних (Big Data), вірту-

альна і доповнена реальність (augmented & additive reality), умови кібербезпеки (cybersecurity), а також соціальні мережі і платформи (Telegram, Facebook), електронні сервіси, які застосовуються в найрізноманітніших сферах людської діяльності – все це створило нові умови, новий «технологічний базис» для зміни традиційних правових інститутів і їх адаптації до нових реалій технологічного існування людства – цифрової екосистеми [1, с. 18].

Трансформація суспільства обумовлена розвитком інформаційного суспільства та поступовим переходом до суспільства знань, впливом цифровізації на всі суспільні процеси. Активне використання цифрових технологій в різних напрямках життєдіяльності зумовило постановку питання про необхідність і достатність прав і свобод людини і громадянина. Наскільки сучасна система прав і свобод людини і громадянина дозволяє забезпечити охорону прав і законних інтересів людини, громадянина, інших суб'єктів права, першочергово до-тичних, а то й вже тісно пов'язаних з цифровими технологіями

Особливо вразливим в епоху цифрової трансформації стає право на приватність, яке є одним із головних прав, які втілюють свободу людини у її негативному розумінні, тобто свободу від втручання ззовні.

Без забезпечення приватності під загрозою опиняються можливості людини будувати власне життя на свій розсуд. Посягання на приватність часто є загрозливими для гідності людини – тієї цінності, яка лежить в основі сучасної системи прав людини [2, с. 29]. З іншого боку, критики приватності розглядають її як право, що виникло не так давно і яке не входить у каталог основних прав.

Новації інформаційного суспільства радикально позначаються на можливості забезпечити приватність. Відомий викривач таємної інформації та противник загального нагляду за людьми Е. Сноуден вважає, що людство втрачає право на приватність, і застерігає, що дитина, яка народжується у наш час, виросте без будь-якого уявлення про приватність та можливість незафіксованої думки [3].

Керівники великих ІТ-корпорацій часто переконані, що приватність є лише ілюзією, та разом із державними чиновниками використовують кожен привід, на зразок терактів 11 вересня, для запровадження чергових систем і стандартів, які знищують приватність [4, с. 25].

У своїй книзі високопосадовці компанії Google розмірковують, що «як і у випадку з суспільним договором, користувачі добровільно відмовляться від своїх цінностей у реальному світі – конфіденційності, безпеки, персональних даних, – щоб скористатися перевагами, що їх дає життя у віртуальному світі» [5, с. 265]

Ті ж люди, які переймаються питаннями приватності, не зареєстровані чи не активні в соціальних мережах та вживають заходів з метою анонімізації в мережі мають багато незручностей і неприємностей. Такий підхід, очевидно, вигідний з огляду на економічні та безпекові інтереси, однак з погляду прав людини викликає обґрунтовані сумніви. Описана проблема є показовою для розуміння того, як нові технології впливають на існуючі баланси індивідуальних, групових і суспільних інтересів, що склалися протягом тривалого часу.

Деякі держави просунулися далі і закріпили «право на цифрову смерть», яке діє за аналогією з заповітом. Французький закон № 2016-1321 від 7 жовтня 2016 року «Про цифрову республіку (державу)» дозволяє громадянам на законодавчому рівні зобов'язати постачальників online-послуг висловити волю громадянина щодо подальшої долі його персональної інформації. На цій основі виникло інше право, безпосередньо пов'язане з цифровізацією суспільства – право на Інтернет, яке розглядається з двох позицій: 1) Інтернет розглядається як послуга в цілому та 2) як право на інформацію, розташовану в Інтернеті. У світовій практиці закріплення цього права здійснюється: визнанням Інтернету універсальною і загальнодоступною послугою (Естонія, Іспанія), закріпленням в конституції права на доступ до Інтернету (Греція, Португалія), визнанням цього права вищими судовими інстанціями (Франція, Коста-Ріка).

Відносно відокремленою групою цифрових прав є права, покликані забезпечити реалізацію конституційних принципів в сфері демократичного устрою нашої держави. Категорія «електронна демократія» міцно входить в сучасний конституційно-правовий вжиток. Активно розробляються форми «електронної» участі громадян в управлінні державними справами (громадські обговорення проєктів нормативно-правових актів, різні види політичної активності, забезпечення системи прямого і зворотного зв'язку між виборцями та обранцями тощо). Окремої уваги в контексті реалізації ви-

борчих прав громадян, а також розробки можливих правомірних способів дистанційного електронного голосування набуває проблема (поки ще не має свого ясного технічного рішення) електронної ідентифікації особи, покликаної спростити виборчу процедуру і підвищити електоральну активність громадян.

Загалом, вплив нових технологій потроху завойовує усі галузі права. Так, очевидні зміни цифрові технології внесли в трудові права особи. В багатьох сферах економіки сучасні технології дозволяють виконувати трудову функцію поза місцем роботи і робочого місця, не тільки вдома (home office), але і на будь-якому місці (mobile office). Від працівника часто очікується, що він повинен бути доступним в будь-який час і на будь-якому місці [6, с. 53]. Якщо в економіках, що розвиваються, це сприймається позитивно як самими працівниками, які бажають більше заробляти, так і споживачами, яким зручно, наприклад, здійснювати покупки в нічний час, то в розвинених країнах традиційні цінності (право на відпочинок і приватне життя) беруть верх. У Франції 8 серпня 2016 року прийнятий Закон «Про працю, модернізацію соціального діалогу та забезпеченні кар'єри» [7], одна з глав якого називається «Адаптація трудового права до цифрової епохи». Вона передбачає право працівника на відключення цифрових пристроїв (телефону та електронної пошти) з метою невтручання в час його відпочинку, відпустки, приватного та сімейного життя. Тобто, в неробочий час французькі працівники мають право не відповідати на дзвінки чи листи роботодавця. І дійсно, у вихідні та святкові дні французи практично «недоступні».

Не менш важливі й права інтелектуальної власності. Цифровий простір і кіберфізичні системи визначають нові виклики для інституту інтелектуальної власності. Нова реальність кіберпростору і кіберпослуг серед інших проблем акцентує увагу на питаннях безпеки використання інтелектуальної власності для всіх учасників цивільного обороту, включаючи самих правовласників. Створення побудованих за принципом комплексних технологій складних об'єктів (штучний інтелект, аналітичні структури на основі Big Data, самоврядні системи за типом Smart Everything тощо) формує запит на розширення переліку охоронюваних об'єктів інтелекту-

альної власності, зміни способів правової охорони в цифровому просторі, створення сегменту цифрових послуг як різновиду об'єктів інтелектуальної власності, створення «кібервласності» (права на віртуальні об'єкти цифрового простору).

Право на освіту сьогодні також активно розвивається в умовах цифровізації. Проблема формування єдиного електронного простору знань і розвитку законодавства в даній сфері, безперечно, є досить актуальною в умовах розвитку інформаційного суспільства. Очевидно, що єдиний електронний простір знань повинен передбачати тісний зв'язок науки, освіти, бібліотечної системи, системи загальнодоступної інформації в мережі Інтернет. Саме на основі формування єдиного електронного простору знань повинен забезпечуватися перехід від інформаційного суспільства до суспільства знань. Інформація та рівень її застосування і доступності кардинальним чином впливають на економічні та соціокультурні умови життя громадян. При цьому переважне значення для розвитку особистості, економіки і держави, в тому числі цифрової економіки та електронної держави, мають отримання, збереження, виробництво і поширення достовірної інформації з урахуванням стратегічних національних пріоритетів.

У сфері підприємницької та іншої економічної діяльності цифрові технології також вносять корективи у права особи, вони здатні автоматизувати правове забезпечення цивільного обороту у так званих смарт-контрактах. Виконуючи укладений договір, наприклад купівлі-продажу, продавець не може бути абсолютно впевнений в тому, що отримає гроші за товар, а покупець не впевнений, що він отримає товар від продавця. Смарт-контракти суттєво змінюють нинішні уявлення про виконання зобов'язань та вплинуть на весь цивільний оборот. Впровадження смарт-контрактів пов'язані з прискореним проникненням у наше життя технології блокчейн, куди можна записувати дати народження людей, фінансові транзакції, відбитки пальців, зберігати відомості про такі документи, як дипломи, паспорти, водійські права тощо [8, с. 168].

Таким чином, можна зробити висновок про те, що права людини еволюціонують разом з розвитком суспільства, держави, цифрових технологій. Виникли нові специфічні цифрові права, які до-

сити важко врегулювати через часткове протиріччя вже усталеним нормам, а також протиріччями, пов'язаними з неможливістю надати повну свободу громадянам в мережі Інтернет.

Покоління прав людини еволюціонують разом з розвитком цифрових технологій. Сфера дії раніше існуючих прав розширюється, з'являються нові права (зокрема, право на доступ до мережі Інтернет). Процес цифровізації незворотній і на сьогодні існує значний масив прогалин в законодавстві, які необхідно врегулювати.

Використана література:

1. Карцхія А. А. Цифровые технологии – правовой аспект. Интеллектуальная собственность. *Промышленная собственность*. 2018. № 10. С. 17-26.

2. Права людини в інформаційному суспільстві : метод. вказівки до вивчення курсу / уклад. П. М. Сухорольський. Львів: Видавництво Львівської політехніки, 2016. 64 с.

3. Сноуден: людство втрачає право на приватність [Електронний ресурс] // Крим. Реалії. Режим доступу: <http://ua.krymr.com/archive/news-uk/20160101/16928/16928.html?id=25345481>

4. Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society / Eds: Ian Kerr, Valerie Steeves, Carole Lucock. Oxford University Press, 2009. 592 p.

5. Шмідт Е. Новий цифровий світ / Ерік Шмідт, Джаред Коен. Львів: Літопис, 2015. 368 с.

6. Чесалина О. В. Работа на основе интернет-платформ (crowdwork и work on demand via apps) как вызов трудовому и социальному праву // Трудовое право в России и за рубежом. 2017. № 1. С. 52–55

7. LOI n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels [Електронний ресурс] // Режим доступу: <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000032983213&fastPos=3&fastReqId=644176944&categorieLien=id&oldAction=rechTexte>

8. Левицька Н. Використання цифрових технологій у праві. Підприємство, господарство і право. 2019. №9. С. 165-169

Кононенко В.В.

доктор історичних наук, професор

ЗАХИСТ ПРАВ ТА СВОБОД ГРОМАДЯН В УМОВАХ ЕЛЕКТРОННОГО УРЯДУВАННЯ

В умовах широкого використання інформаційних технологій змінюються підходи до механізмів, засобів та форм публічного управління. Інтернет є не тільки невід'ємним елементом життя людини, а й сучасною ознакою діяльності органів державної влади, органів місцевого самоврядування та інших суб'єктів, що виконують функції публічного управління.

У вересні 2017 р. Кабінетом Міністрів України було прийнято «Концепцію розвитку електронного урядування в Україні». У ній визначено, що розвиток електронного урядування є одним з першочергових пріоритетів реформування системи державного управління. Концепція визначає електронне урядування як форму організації державного управління, яка сприяє підвищенню ефективності, відкритості та прозорості діяльності органів державної влади та органів місцевого самоврядування з використанням інформаційно-телекомунікаційних технологій для формування нового типу держави, орієнтованої на задоволення потреб громадян [1]. Отже, в основі електронного урядування (e-government) лежить використання інформаційно-комунікаційних технологій (ІКТ) як інструменту підтримки розвитку належного врядування, підвищення рівня ефективності та результативності виконання урядових завдань, покращення процедур з надання публічних послуг, використання інформації при прийнятті рішень, забезпечення ефективного зв'язку як між суб'єктами влади, так і між владою та громадянами. Головна мета цих процесів забезпечити динамічні та стійкі відносини між владою та громадянами, а кінцевою метою мають стати задоволення потреб громадян та суспільства. Саме «клієнт-орієнтованість» публічних інститутів, сприйняття громадян як споживачів адміністративних, публічних послуг і прийняття підходів задоволення очікувань споживачів, є в основі електронного урядування [2, с. 30].

З одного боку, активне використання ІКТ вже сприятиме ефективнішому реалізації та захисту прав та свобод громадян, оскільки електронне урядування, як зазначено в Концепції «дасть змогу створити додаткові механізми реалізації права на доступ до інформації, що перебуває у володінні органів влади, підвищити прозорість діяльності таких органів, забезпечить вільний обіг інформації та можливість її подальшого використання з метою реалізації особистих прав та свобод людини і громадянина» [1]. З іншого – застосування ІКТ веде до розвитку інфраструктури електронної ідентифікації, електронного документообігу, накопичення інформації клієнтів електронних послуг, що у свою чергу створює проблему захисту персональних даних. Ідентифікаційні дані фізичної особи підпадають під визначення персональних даних, оскільки відповідно до Закону України «Про захист персональних даних» (2010 р.) «персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [3, с. 481].

Закон України «Про захист персональних даних» прямо вказує, що використання персональних даних володільцем можливе лише відповідно до їхніх професійних чи службових або трудових обов'язків. У той же час законом чітко зазначено, що «використання персональних даних володільцем здійснюється у разі створення ним умов для захисту цих даних» [3, с. 481]. Тобто закон України чітко передбачає, що володільць (розпорядник) ідентифікаційних даних особи можуть використовувати ці дані з дотриманням режиму захисту, збереження та їх нерозголошення.

Саме на цій стадії роботи з персональною інформацією спостерігаємо суттєві недоліки. Сьогодні зафіксовані порушення у сфері розпорядження персональними даними окремими органами державної влади та місцевого самоврядування, установами та організаціями. С. Єсімов, зазначає, що у більшості випадків порушником є оператор персональних даних – державний орган, орган місцевого самоврядування, юридична або фізична особа, що організують і здійснюють обробку персональних даних, визначають цілі та зміст обробки персональних даних [4, с. 153]. Наприклад, як зазначає І. Костенко, в службовій діяльності Національної поліції пошире-

ними є порушення положень чинного законодавства у сфері зберігання й обробки персональних даних про особу, з-поміж яких неналежний захист баз персональних даних [5, с. 297].

У щорічній доповіді Уповноваженого Верховної Ради України з прав людини за 2019 р. про стан додержання та захисту прав і свобод людини і громадянина в Україні зазначено, що «найбільше порушень права особи на захист персональних даних фіксувались у сферах фінансових і банківських послуг, страхування, житлово-комунальних послуг, охорони здоров'я, соціального захисту, освіти, а також при обробці персональних даних під час здійснення відеоспостереження, обліку адміністративних та кримінальних правопорушень» [6, с. 193]. Загалом протягом 2019 р. секретаріат Уповноваженого розглянув 1061 повідомлення про порушення у сфері захисту персональних даних [6, с. 193].

Особливо загрозливими стали порушення щодо збереження, використання, захисту персональних даних у діяльності банків та інших фінансових установ. З огляду на це, Національний Банк України звернувся з листом № 25-0007/11290 «Про недопустимість неправомірного використання персональних даних» від 26 лютого 2018 р. до банківських установ, де вказав на необхідність забезпечення безумовно належної ідентифікації і верифікації клієнтів (представників клієнтів) та зберігання документів, що містять персональні дані [7, с. 193].

13 травня 2020 р. Державне бюро розслідувань повідомило про початок досудового розслідування за фактом витоку інформації, що містила персональні дані громадян України та була розповсюджена в одному із анонімних телеграм каналів. Як зазначає ДБР, за попередньою інформацією, до витоку персональних даних можуть бути причетні посадові особи Головного сервісного центру МВС України та Державної міграційної служби [8]. Очевидно мова йде про мережу Telegram, у якій з'явилося декілька каналів, з яких зливали персональну інформацію. Так, у Telegram з'явився бот, який називається UA Baза, що видавав персональні дані та документи українців. Зокрема, у відкритий доступ потрапили 26 мільйонів посвідчень водія.

На нашу думку, є декілька основних недоліків організації роботи в умовах електронного врядування, що ведуть до порушення

прав та свобод громадян при користуванні ідентифікаційними даними. Серед них:

- збирання, обробка та поширення даних про фізичну особу, які є конфіденційною інформацією, без її згоди;
- порушення вимог при поширенні (розповсюдженні, реалізації, передачі) відомостей про фізичну особу;
- порушення умов зберігання персональних даних та відповідного режиму доступу до них;
- неправомірне передавання персональних даних третім особам.

Варто зазначити, що причини порушень прав та свобод громадян в умовах електронного врядування різні. Основними серед них є: недоліки захисту інформації, що зберігається на комп'ютерах, автоматизованих системах, комп'ютерних мережах, на носіях такої інформації та баз даних державних органів, органів місцевого самоврядування та інших суб'єктів надання публічних послуг; халатність, непрофесійність службовців та посадових осіб, що працюють з інформацією; навмисні порушення режиму обробки, зберігання, поширення та захисту інформації тощо.

Зрозуміло, що усі зазначені недоліки у цій сфері потребують негайного виправлення, а вся робота з персональною інформацією має відповідати певним принципам:

- законності та справедливості;
- легітимної мети;
- пропорційності персональних даних щодо легітимної мети;
- точності (достовірності), актуальності персональних даних;
- обробка персональних даних у формі, що допускає ідентифікацію фізичної особи, якої вони стосуються, не довше, ніж це необхідно для законних цілей, у яких вони збиралися або надалі оброблялися [9, с. 20-21].

Окрім того вважаємо, що й самі громадяни мають дбати про свою безпеку. Свої персональні дані вони мають передавати лише у випадках визначених нормативно-правовими актами України та усвідомленням того, кому вони передають свої ідентифікаційні дані та з якою метою вони можуть бути використані.

Для національного законодавства дороговказом має стати директива ЄС Європейського Парламенту та Ради «Про захист фізич-

них осіб при обробці персональних даних і про вільне переміщення таких даних» від 24 жовтня 1995 р. Цей нормативно-правовий акт є найбільш сучасним документом, який встановлює вимоги щодо того, як має бути організована система захисту персональних даних у державі [10, с. 17].

Таким чином, вважаємо, що із запровадженням електронного урядування перед громадянами відкриваються широкі можливості з реалізації прав та свобод. Електронне врядування має бути орієнтоване, насамперед, на забезпечення прозорості публічного управління та на задоволення потреб громадян через розширення можливостей надання адміністративних та публічних послуг через інформаційно-комунікаційні технології. Проте одночасно, це вимагає постійної роботи щодо захисту персональних даних громадян, оскільки будь-яка адміністративна чи інша публічна послуга пов'язана із ідентифікацією особи, а отже із збиранням інформації про неї. Саме тому, органи державної влади та органи місцевого самоврядування, організації та установи мають використовувати отриману інформацію лише відповідно до функцій та завдань, які перед ними стоять, та лише у тій мірі, наскільки це необхідно для надання послуги. Режим збереження та захисту отриманої інформації при наданні публічних послуг має стати невід'ємною рисою їх діяльності.

Список використаної літератури:

1. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку електронного урядування в Україні» від 20 вересня 2017 р. // Верховна Рада України. – Режим доступу: <http://zakon2.rada.gov.ua/laws/show/649-2017-%D1%80>.
2. Погребняк І. Електронний уряд (e-government) і електронне урядування (e-governance): поняття та принципи функціонування / І. Погребняк // Право та інновації. – 2014. – № 3 (7). – С. 26-35.
3. Закон України «Про захист персональних даних» від 1 червня 2010 р. // Відомості Верховної Ради України. – 2010. – № 34. – С. 481.
4. Єсімов С. С. Особливості правового режиму інформаційних систем з обробки персональних даних / С. С. Єсімов // Науковий вісник Львівського державного університету внутрішніх справ. – 2018. – № 1. – С. 145-156.

5. Костенко І. В. Проблеми правового захисту персональних даних у діяльності Національної поліції / І. В. Костенко // Юридичний часопис Національної академії внутрішніх справ. – 2018. – № 1 (15). – С. 296-303.

6. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини за 2019 р. про стан додержання та захисту прав і свобод людини і громадянина в Україні // Державна прикордонна служба України. – Режим доступу: https://dpsu.gov.ua/upload/zvit_za_2019.pdf.

7. Лист НБУ № 25-0007/11290 «Про недопустимість неправомірного використання персональних даних» від 26 лютого 2018 р. // Все про бухгалтерський облік. – Режим доступу: <http://vobu.ua/ukr/documents/item/lyst-nbu-vid-260218-r-25-0007-11290-pro-nedopustymist-nepravomirnoho-vykorystannia-personalnykh-danykh>.

8. ДБР розслідує причетність посадовців МВС та ДМС до витоку персональних даних громадян // Державне бюро розслідувань. – Режим доступу: <https://dbr.gov.ua/news/dbr-rozslidue-prichetnist-posadovciv-mvs-ta-dms-do-vitoku-personalnikh-danikh-gromadyan>.

9. Стандарти захисту персональних даних в соціальній сфері / М. В. Бем., І. М. Городиський. – Львів: б.в., 2018. – 110 с.

10. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. – К.: К.І.С., 2015. – 220 с.

Маньгора В.В.

кандидат педагогічних наук, доцент,
професор кафедри права ПрАТ
«Вищий навчальний заклад «МАУП»
Вінницького інституту

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ КІБЕРБУЛІНГУ В СУЧАСНИХ УМОВАХ

З метою протидії поширенню коронавірусної інфекційної хвороби COVID-19 навчально-виховний процес проходить дистанційно. Виконання завдань освіти потребує використання учасниками освітнього процесу інформаційно-комунікаційних технологій. Однак реалізація права на освіту, права на свободу вираження думки та інформації пов'язана з ризиками.

Типи небезпеки, яка загрожує дітям в Інтернеті:

- загроза особистій безпеці: спілкування зі незнайомими людьми або залучення до протиправних дій;
- безпека інших: кібербулінг, вчинення злочинів, посягання на безпеку оточення;
- витік персональної інформації - розголошення номерів кредитних карток, номерів телефонів та небезпека завантаження шкідливих програм [1].

Самоізоляція, дистанційне навчання, збільшення часу спілкування в Інтернеті, не завжди можливість контролювати дітей батьками, не знання правил безпеки в мережі може призвести до ситуації кібербулінгу.

Кібербулінг - це знущання, приниження, агресивні напади, які здійснюють за допомогою різних гаджетів (зокрема телефонів), з використанням Інтернету, будь-яких електронних (цифрових) технологій [2].

За даними ЮНІСЕФ у 2018 р. кожен п'ятий підліток визнав, що ображав однолітків в онлайн-просторі. «Жертвами» онлайн-знущань визнала себе п'ята частина опитуваних – 21,5% [3]. За умови коронавірусної інфекційної хвороби COVID-19 випадків кібербулінгу стало більше.

Ознаки кібербулінгу можуть включати:

- емоційне пригнічення під час або після використання Інтернету або телефону;
- приховування певних фактів свого Інтернет спілкування;
- уникання шкільних або дружніх зустрічей;
- приступи немотивованого гніву дома;
- зміна настрою, поведінки, сну або апетиту;
- бажання припинити користуватися комп'ютером або мобільним телефоном;
- уникання розмов про діяльність комп'ютера або мобільних телефонів [4].

Дж. Хейвард вважає, що кібер-залякування може включати:

- 1) надсилання недоброзичливих текстових повідомлень, електронної пошти та повідомлень у чаті;
- 2) переадресацію конфіденційних листів електронною поштою, текстових повідомлень або повідомлень у чаті іншим учням;
- 3) дошкуляння учневі злосливими текстовими повідомленнями;
- 4) відкриття принизливого веб-сайту або сторінки профілю про учня та запрошення інших до коментарів;

5) використання камери мобільного телефону для зняття відео або фотографування учня з метою його компрометування [5, с. 195].

Наприкінці 2018 р. український парламент ухвалив Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» [6]. Цей Закон вніс зміни до Кодексу України про адміністративні правопорушення № 8073-1-X від 07 грудня 1984 р. (далі – КУпАП) та Закону України «Про освіту» № 2145-VIII від 05 вересня 2017 р., доповнивши їх статтями про булінг. Було законодавчо визначено поняття «булінг» та його основних ознак. Так, булінг (цькування) визначається як діяння (дії або бездіяльність) учасників освітнього процесу, які полягають у психологічному, фізичному, економічному, сексуальному насильстві, зокрема із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи та (або) такою особою стосовно інших учасників освітнього процесу, унаслідок чого могла бути чи була завдана шкода психічному або фізичному здоров'ю потерпілого [7]. Сучасне законодавство

не застосовує поняття «кібербулінг», а використовує термін засоби електронних комунікацій.

Визначення поняття кібербулінгу як протиправного діяння та встановлення відповідальності за його вияви (форми) в Україні на сучасному етапі в науковій та законодавчій сферах не сформульовано. Однак деякі його вияви є вкрай небезпечними та можуть призвести як різновид булінгу до тяжких наслідків, пов'язаних зі шкодою для здоров'я та життя осіб [8, с. 282].

КУпАП був доповнений статтею 173-4 яка передбачає що до відповідальності притягуються учасники освітнього процесу, а в разі якщо діяння вчиняють неповнолітні та малолітні, то відповідальність нестимуть батьки або особи що їх замінюють накладанням штрафу від 50 до 100 неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від 20 до 40 годин. Якщо цькування було вчинене групою осіб або повторно протягом року після накладення адміністративного стягнення – це тягне за собою накладення штрафу від 100 до 200 таких мінімумів або громадські роботи на строк від 40 до 60 годин. Для притягнення до відповідальності винної особи слід звернутися до керівника навчального закладу або до Національної поліції України. КУпАП встановлює адміністративну відповідальність у вигляді штрафу від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян або громадські роботи на строк від двадцяти до сорока годин за вчинення булінгу [9].

Максимальна сума відповідальності – 3400 гривень, мінімальний штраф – 850 гривень. За неповідомлення керівником закладу освіти уповноваженим підрозділам органів Національної поліції про випадки цькування передбачений штраф від 850 до 1700 гривень або призначать виправні роботи на строк до одного місяця з відрахуванням до 20 % заробітку.

В. Петрук вказує на деякі особливості притягнення до адміністративної відповідальності за булінг. До адміністративної відповідальності можна притягнути тільки учасника освітнього процесу, при цьому принаймні одна зі сторін має бути неповнолітньою. Другий важливий аспект – що жертві такої поведінки або свідкам потрібно повідомити про це керівництво школи. У випадку, якщо дитина школі не довіряє, боїться, що її засміють, вона може напря-

му звернутися до поліції, написавши заяву про вчинення щодо неї адміністративного правопорушення. Але поліція, якщо дійде висновку, що дійсно відбувалося цькування, все одно буде звертатися до керівництва школи [10].

Норми Закону України № 2657-VIII «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)» встановлюють адміністративну відповідальність і не передбачають внесення змін до Кримінального кодексу України стосовно запровадження кримінальної відповідальності за скоєння правопорушень, пов'язаних з булінгом (цькуванням), оскільки скоєння правопорушником при вчиненні булінгу (цькування) інших дій, кваліфікуються відповідними статтями Кримінального кодексу України [6].

Безпосередньо цькування (булінг) має наслідком лише адміністративну відповідальність для неповнолітніх осіб. Однак у тих випадках, коли булінг має фізичний характер і завдає шкоди здоров'ю людини, окрім КУпАП, до кривдника застосовується Кримінальний кодекс України, особу може бути притягнуто до кримінальної відповідальності і з 14 років (за умисне вбивство, умисне тяжке або середньої тяжкості тілесне ушкодження, доведення до самогубства, хуліганство, катування).

Найчастіше дії кібербулерів кваліфікують як хуліганство (ст. 296 КК України). У разі встановлення факту скоєння неправомірної дії у віртуальному просторі (кібербулінг), відповідальність покладається на власника технічного пристрою, за допомогою якого було вчинено певну неправомірну дію [11, с. 173].

На сьогоднішній день є дані судової практики. Перше рішення по булінгу (кібербулінгу) було винесено суддею Бориспільського міськрайонного суду Київської області 05 лютого 2019 року.

За фактом булінгу було складено протокол про адміністративне правопорушення і скеровано на розгляд до суду, який власне і встановив факт булінгу, тобто дії психологічного і сексуального насильства із застосуванням засобів електронних комунікацій, що проявилось у висвітленні непристойних фото в мережі «Інстаграм», в результаті чого могло бути завдано шкоди психічному здоров'ю потерпілої. Зазначало, що в судовому засіданні мати неповнолітньої провини у скоєному визнала. За рішенням суду у цій справі суд на-

клав на батьків винної особи покарання у вигляді штрафу в розмірі 50 неоподатковуваних мінімумів доходів громадян, що становить 850 грн, і судовий збір у розмірі 384,20 грн. [12].

Справи, що полягають у булінгу шляхом використання сучасних інтернет технологій, не містять належних електронних доказів, як наслідок, відповідальність настає виключно у разі визнання вини учасником процесу. Вже наявна судова практика вказує на різноманіття доказової бази, яка може як допомогти притягнути до відповідальності, так і звільнити від відповідальності.

Розвиток інформаційно-комунікаційних технологій, збільшення випадків агресивної поведінки в Інтернеті під час карантину серед учасників освітнього процесу потребує прийняття нових нормативно-правових актів, внесення змін до діючих відповідно до міжнародних стандартів та іноземного досвіду. Нагальною потребою є визначення поняття «кібербулінг», визначити ознаки, види, форми, юридичну відповідальність на законодавчому рівні. Враховуючи досвід іноземних країн, розуміючи, що інформаційно-комунікаційні технології в сучасних умовах є невід'ємною частиною життя, і їх роль постійно зростає необхідно прийняти закон, який би гарантував захист від кібербулінгу, встановлював правовий механізм протидії кібербулінгу, передбачав дієву процедуру внесення змін відповідно до швидкого розвитку інформаційно-комунікаційних технологій та інформаційно-правових відносин.

Розв'язанню проблеми кібербулінгу повинні сприяти відповідні державні органи, батьки, заклади освіти, педагоги, інститути громадянського суспільства, які можуть долучитися до протидії насильству над дітьми. Освітні навчальні плани мають включати окремі спецкурси з медіа-грамотності та інформаційної безпеки. Профілактика кібербулінгу є найефективнішим способом, адже вона попереджає, його негативні наслідки.

Література

1. У МВС розповіли, як дітям безпечно «залипати» в гаджетах на час карантину. URL:<https://hromadske.ua/posts/u-mvs-rozpovili-yak-dityam-bezpechno-zalipati-v-gadzhetah-na-chas-karantinu> (дата звернення: 14.05.2020).

2. Види булінгу та кібербулінгу. URL:<https://edu.bullyingstop.org.ua/article/4> (дата звернення: 14.05.2020).

3. ЮНІСЕФ: Українські підлітки нехтують своїм здоров'ям, погано харчуються та проводять життя в соціальних мережах. URL: <https://www.unicef.org/ukraine> (дата звернення: 14.05.2020).

4. Що таке кібер-булінг. URL: <https://klepkainfo.com/zdorovya/kiber-buling-viznachennya-oznaki-metodi.html> (дата звернення: 14.05.2020).

5. Хейвард Дж. Закони проти кібер-залякування: загроза для свободи слова учнів. Право США. 2013. № 1-2. С. 194-206. URL: http://nbuv.gov.ua/UJRN/prccha_2013_1-2_15 (дата звернення: 14.05.2020).

6. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) : Закон України від 18 грудня 2018 р. № 2657-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2657-19> (дата звернення: 14.05.2020).

7. Про освіту : Закон України від 5 вересня 2017 р. № 2145-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2145-19> (дата звернення: 14.05.2020).

8. Миронюк Т. В., Запорожець А. К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 2. С. 275–284.

9. Кодекс України про адміністративні правопорушення від 7 грудня 1984 р. № 8073-X. *Відомості Верховної Ради Української РСР*. 1984. Додаток до № 51. Ст. 1122.

10. Хто заплатить за кібербулінг: український досвід. <https://www.radiosvoboda.org/a/khto-zaplatyt-za-kiberbuling/30123790.html> (дата звернення: 14.05.2020).

11. Нестеренко А. Адміністративно-правова протидія кібербулінгу стосовно дітей. *Вісник Національного університету «Львівська політехніка»*. 2019. Випуск 6. Юридичні науки. № 911 (21). С. 170-175.

12. В Україні винесено перше судове рішення за фактом булінгу в школі. URL: https://ukr.lb.ua/society/2019/02/12/419612_ukraini_vineseno_pershe_sudove.html (дата звернення: 14.05.2020).

13. Гомзяк І. Правозастосовна практика стосовно булінгу: що необхідно знати правозахиснику. URL: <http://zakon1.rada.gov.ua/laws/show/254к/96-вр>. (дата звернення 15.05.2020).

Проць І.М.

кандидат юридичних наук,
доцент кафедри адміністративно-
правових дисциплін Львівського
державного університету внутріш-
ніх справ

**ТЕНДЕНЦІЇ РОЗВИТКУ ТЕХНОЛОГІЙ ДИСТАНЦІЙНОГО
БАНКІВСЬКОГО ОБСЛУГОВУВАННЯ В УКРАЇНІ**

Розвиток інформаційних технологій забезпечило динамічний розвиток дистанційного банківського обслуговування клієнтів в Україні. Дистанційне банківське обслуговування включає всі можливі способи надання банківських продуктів і послуг юридичним та фізичним особам з використанням засобів комунікацій, які не вимагають безпосереднього візиту клієнта в банк. При взаємодії з фізичними особами цей тип послуг помітно розширює клієнтуру банку та збільшує інтенсивність операцій: кредитних, депозитних, платіжних.

На рівні юридичних осіб дистанційне банківське обслуговування забезпечує сталий розвиток взаємодіючих на ринку суб'єктів різних сфер діяльності – фінансової, виробничої, торговельної.

У контексті використання технологій у даний час прийнято виділяти наступні види дистанційного банківського обслуговування:

- «банк-клієнт» (на комп'ютері користувача банком встановлюється спеціальна програма-клієнт, взаємодія з комп'ютером банку може здійснюватися за доступними каналами зв'язку);

- Інтернет-банкінг (здійснюється за допомогою стандартного веб-браузера без установки спеціальної банківської програми на комп'ютер клієнта);

- мобільний банкінг (надання послуг клієнту з використанням телефонного зв'язку);

- зовнішні сервіси (включають технології дистанційного банківського обслуговування з використанням пристроїв банківського самообслуговування – банкоматів і платіжних терміналів).

Асортимент доступних банківських продуктів, пропонує в у межах дистанційного банківського обслуговування в режимі

online, постійно розширюється та стає різноманітним. Він включає такі опції, як віддалене управління рахунками через систему клієнт-банк і Інтернет-банк, системи mobile bank, можливість через телефонний центр банку здійснити подачу заявки на виготовлення банківських, підключення нових послуг і сервісів.

У всіх банках України клієнт може перевіряти стан поточного рахунку, здійснювати грошові перекази, оплачувати електронні рахунки. Більш складні системи дозволяють клієнтам в online-режимі скласти заявку на отримання кредиту, отримати повну інформацію щодо рахунків, ініціювати випуск додаткової банківської карти відкрити строковий депозит, збільшити кредитний ліміт і змінити PIN-код.

До цього класу обслуговування для юридичних осіб відносяться пакетне зарахування заробітної плати на карт-рахунки співробітників, подача заяв на отримання платіжних карт. Поширення подібних послуг сприяє розвитку координаційних зв'язків організації та застосування процесного підходу.

Виник цілий шар банківської клієнтури, для якої системи дистанційного банківського обслуговування стали більш звичними засобами зв'язку з кредитними організаціями. Як правило, це люди працездатного віку, від 20 до 50 років, що сформували позитивну думку про зручність і безпеку мобільного та Інтернет-зв'язку для проведення операцій з власними фінансами.

Здешевлення мобільних пристроїв зв'язку та тарифів стільникових операторів створили можливості для бурхливого розвитку роздрібного банківського обслуговування в сфері мобільного банкінгу. Основна перевага полягає в зручності, оскільки дистанційно керувати рахунками клієнт може зі звичайного комп'ютера, не обмежуючи себе ні територіально, ні в часі.

Дистанційне банківське обслуговування в комерційних банках України має ряд недоліків: недостатня розвиненість законодавчого регулювання, високі витрати на створення, впровадження і обслуговування систем дистанційного банківського обслуговування, проблеми технологічного характеру, наявність різного роду ризиків, це уповільнює процес розвитку дистанційного банківського обслуговування в банківській системі України.

Система Інтернет-банкінгу вимагає значних фінансових, людських, інтелектуальних витрат на її розробку, впровадження та постійну підтримку, що робить можливим повноцінне використання переважно у великих банках («ПриватБанк» (Приват24), «Ощадбанк» (Ощад 24/7), тощо). В більшості невеликих банків або система дистанційного обслуговування Інтернет-банкінг відсутня, або її можливості поки що зводяться лише до послуг з відкриття депозиту та переказу коштів [1, с. 176-177].

Розвиток технологічних та фінансових інновацій зумовив появу нефінансових компаній, які надають традиційні фінансові послуги (галузь фінтех (FinTech – скорочене від «financial technology», тобто фінансова технологія). Впродовж останніх трьох років FinTech активно розвивається в Україні, де зараз на ринку активно працюють 80 компаній. Наймасовіший ринковий сегмент в українському FinTech становлять платежі та грошові перекази. В цій сфері працює понад 30% усіх стартапів [2, с. 42].

Банки постійно відстежують новації на ринку дистанційного банківського обслуговування, в тому числі у сфері ризиків шахрайства. Це обумовлено тим, що з кожним роком кількість шахрайських і хакерських атак в системах дистанційного банківського обслуговування зростає. Банки змушені купувати або розробляти нові захисні програми від подібних злочинів, що характерно для організацій, що дистанційно діють у всіх суспільних сферах.

Цифровий банкінг може бути визначений як розширення транзакційних об'єктів для клієнтів банками через різні захищені цифрові канали, піклуючись про безпеку даних, пов'язані з ними зниження ризиків та регуляторні аспекти самими банками. Це досягається шляхом інтеграції онлайн (Інтернет) та мобільних банківських послуг шляхом впровадження новітніх цифрових технологій, таких як аналітика, соціальні медіа, інноваційні платіжні рішення та мобільні технології з метою перевищення очікувань клієнтів, зручності та досвіду [3, с. 22].

Залишається невирішеною частина проблем розвитку, яких не позбавлена жодна сфера діяльності підприємства, зацікавленого в розширенні позицій на ринку товарів і послуг, з цією метою банки змінюють організаційну структуру та функціональне наповнення.

Впроваджуючи інновацій в системи дистанційного банківського обслуговування, комерційні банки України намітили певний вектор розвитку. Наприклад, важливою інновацією став доступ до оплати постачальника послуг за штрих-кодм через мобільний додаток, хоча поки це нововведення є тільки для пристроїв, сумісних з iPhone. Однак, такі послуги дистанційного банківського обслуговування стануть доступні для інших типах пристроїв.

Не менш значущими інноваціями для корпоративних клієнтів стали послуги RFM - інструменти управління та планування фінансів, щоб забезпечити аналіз діяльності компанії та надання результатів у вигляді графіків (у розрізах контрагентів, статей бюджету або періодів діяльності компанії). Це дозволило клієнтам оперативно приймати рішення щодо веденню бізнесу та контролю за фінансовими потоками.

До переваг, які забезпечуються розвитком дистанційного банківського обслуговування відносяться нові стратегії роздрібного бізнесу, що спираються на концепцію дистанційного банківського самообслуговування клієнтів. Клієнту достатньо один раз відвідати відділення банку для укладення договору.

Опитування різних компаній, що забезпечують технології для здійснення Інтернет-банкінгу показало, що більше половини банків мають розвинені системи дистанційного банківського обслуговування.

В Україні комерційні банки пропонують досить широкий спектр послуг (більш 250 найменувань), серед яких послуги електронного банкінгу набирають популярність. У країнах ЄС рівень розвитку дистанційного банківського обслуговування, забезпечує можливість надання клієнту комплексного набору банківських послуг незалежно від географічного положення філії банку, в якому обслуговується клієнт, або використовуваного клієнтом каналу доступу до банківського обслуговування.

Послуги дистанційного банківського обслуговування пропонуються на більш вигідних умовах, ніж якби вони були придбані при особистому зверненні. Клієнту пропонується пакет з безлічі каналів здійснення дистанційного банківського обслуговування / Якщо раніше банки пропонували клієнтам сервіси, то зараз вони

намагаються потрапити в середовище клієнта (мобільні пристрої, соціальні мережі, інформаційні сервіси), розміщуючи сервіси в тих каналах, де потенційно можуть бути затребувані клієнтами.

Дослідники з KPMG вважають, що банки та фінансові організації у перспективі використовуватимуть кожен крок користувачів для цілкового розуміння життя та потреб клієнтів і персоналізації запропонованих послуг за допомогою штучного інтелекту. Роль банку полягатиме в тому, щоб визначити та запропонувати клієнту найбільш релевантний наразі сервіс, замовити та забезпечити його оплату. Взаємодія з клієнтами буде максимально простою та зручною за допомогою голосу, біометрії та *wearable devices*, а оцінка ризикованості позичальника ґрунтуватиметься на життєвих звичках та історії покупок [4].

Список використаної літератури

1. Захаркін О. О. Роль інтернет-банкінгу в розвитку ринку фінансових послуг / Захаркін О. О., Захаркіна Л. С., Авраменко М. О. *Гроші, фінанси і кредит*. 2017. № 25. С. 173-177.
2. Шевчук Ю. В. Оцінка використання фінансових інновацій на фінансовому ринку України / Ю. В. Шевчук. *Економіка та держава*. 2019. № 5. С. 39-44.
3. Інновації в банкінгу: чому не всі банки помруть, але всі знають змін. *Mind*. 30 вересня 2019 року. URL. <https://mind.ua/publications/20202666-innovaciyi-v-bankingu-chomu-ne-vsi-banki-pomrut-ale-vsi-zaznayut-zmin>
4. Проблеми та перспективи розвитку цифрового банкінгу. 04.2019. URL.<http://khibs.ubs.edu.ua/wp-content/uploads/2019/04/Tishenko.pdf>

Доронін І.М.

кандидат юридичних наук, доцент
зав. наукової лабораторії НДІІ
інформатики і права,

**ІНТЕРЕСИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ,
ЯК ПІДСТАВА ДЛЯ ОБМЕЖЕННЯ ПРАВ І СВОБОД
ЛЮДИНИ, У СУЧАСНОМУ
ПОЛІТИКО-ПРАВОВОМУ КОНТЕКСТІ**

Проблематика загального визначення можливих підстав для обмеження прав і свобод людини залишається актуальною у правовій науці протягом тривалого часу. Чинні міжнародно-правові акти з питань захисту прав і свобод людини визначають наявність існування як підстави для їх обмеження у певних випадках у тому числі «інтересів національної безпеки».

Так, статтями 8, 10, 11 Конвенції про захист прав людини і основоположних свобод (далі – Конвенція) передбачено, що право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції, право на свободу вираження поглядів і право на свободу зібрань та об'єднання може бути обмежене у певних випадках. Загальне формулювання підстав для обмеження може розумітись як наявність випадків, коли обмеження (втручання) здійснюється згідно із законом, і є необхідним у демократичному суспільстві в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушення чи злочинам. Необхідність для демократичного суспільства зумовлена існуванням певних інтересів, що ототожнюються із національною та громадською безпекою. Формулювання «інтересів національної безпеки» у тексті конвенції прямо не ототожнюється із політикою боротьби зі злочинністю, тобто розглядається як окреме поняття. Водночас має місце і доволі широке трактування термінів «запобігання заворушенням» також і у контексті вчинення правомірних дій для «придушення заворушення» або «повстання» (у ст. 2 Конвенції щодо виключень стосовно права на життя).

Отже, тлумачення тексту Конвенції дає змогу визначити низку термінів, які ототожнюються із підставами (випадками) для обмеження прав і свобод людини і можуть розумітись доволі широко. Мова йде про «національну безпеку», «громадську безпеку», а також «запобігання заворушенням». Оскільки визначень для термінів у тексті Конвенції не наводиться, відповідне розуміння формується юридичною, насамперед судовою, практикою.

Аналіз судової практики Європейського суду з прав людини (ЄСПЛ) передусім свідчить про наявність певних усталених підходів щодо загального розуміння «інтересу» – інтересу держави, як суб'єкта правовідносин. Такий інтерес є підставою для обмежувальних дій органів держави стосовно конкретної особи у певних обставинах. Найчастіше контекст «інтересів національної безпеки» згадується у випадках порушення прав людини, визначених ст. 8, 10 та 11 Конвенції, хоча, на нашу думку, застосування зазначеного поняття є дещо ширше і може розглядатись у справах стосовно порушень інших визначених Конвенцією прав людини (у тому числі, - і статтею 2).

Мова йде про право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції, право на свободу вираження поглядів, право на свободу мирних зібрань і свободу об'єднання з іншими особами, а також про право на життя.

Насамперед, слід визнати, що обмеження прав допускається тільки згідно з вимогами закону – тобто законодавчого акту, якій повинен мати загальні ознаки детальності, передбачуваності та доступності. Зазначене положення кореспондується із вимогами вітчизняного законодавства, зокрема, з приписами ст. 19 Конституції України.

Поняття «національної безпеки», що в принципі відомо як законодавству України так і у юридичній науці і має відповідні дефініції, розглядається у практиці ЄСПЛ на рівні принципів. Тобто має місце уникнення дефініції, оскільки її надання може ускладнити сприйняття положень міжнародно-правового акту. Так, Комісія (ЄСПЛ) у рішенні у справі «*Esbest v United Kingdom*» від 02.04.1993 відзначила, що надання всебічної дефініції поняттю «національна безпека» для вирішення конкретної ситуації не є обов'язковим.

Таким чином, держава позбавлена необхідності визначати дефініцію, зазначене питання віддається на розсуд тієї чи іншої правової системи. Водночас, законодавство, що регламентує забезпечення національної безпеки, повинно відповідати загальним ознакам деталістості, передбачуваності та доступності, а також відповідати принципам та загальним підходам щодо захисту прав людини.

Вітчизняне законодавство традиційно містить доволі широкі дефініції для терміну «національна безпека». При цьому дефініція, яка діяла протягом 2010-2017 років (ст. 1 Закону України «Про основи національної безпеки України» в редакції відповідно до змін внесених Законом України від 01.07.2010) була занадто широкою і охоплювала практично всі напрями державної політики та суспільного життя. За такого розуміння інтереси національної безпеки мали по суті необмежений для можливого тлумачення характер, що зумовлювало тенденцію до порушення гарантованих прав і свобод людини. Чинний Закон України «Про національну безпеку України» у визначенні поняття «національна безпека» дещо конкретизував розуміння національної безпеки. Водночас законодавець вдався до іншого заширокого трактування – у розумінні «національних інтересів».

Таким чином, визначаючи певний обсяг для поняття, у першу чергу варто зосередитись на тих умовах, що зазвичай стосуються суті державної діяльності, як спрямована на забезпечення національну безпеку. Аналіз судової практики ЄСПЛ з цього приводу дає змогу визначити, що мова йде про державну діяльність, спрямовану на захист державного суверенітету, територіальної цілісності, державного устрою відповідної країни. Тому в основному мова йде про протидію окремим загрозам у вигляді діяльності окремих осіб (груп, інших держав), що посягає на інтереси у зазначених вище напрямках. Як правило, посилення на інтереси громадської безпеки має місце у випадках протидії злочинності так би мовити «загальнокримінального» характеру. Інтереси національної безпеки в основному згадується у контексті протидії розвідувально-підбивної діяльності іноземних держав, або терористичній діяльності. Так, знакові судові справи ЄСПЛ щодо обмеження прав людини в інтересах національної безпеки стосуються саме таких

обставин. У відомій справі *Amann v Switzerland* мова йде про діяльність швейцарського державного органу щодо тривалого таємного спостереження за особою та накопичення здобутої інформації в інтересах протидії розвідувально-підбивній діяльності. Таке рішення зумовлено наявністю телефонного контакту посольства колишнього СРСР з особою-заявником, що на думку контррозвідувального органу мало ознаки прихованого спілкування. Швейцарія не надала суду докази щодо підтвердження прихованості спілкування або співробітництва особи з іноземною розвідкою, ніякі інші дії щодо притягнення особи до кримінальної відповідальності або висунення щодо неї юридичних підозр також не проводились. Також не було ніяких доказів ведення конкретним іноземним дипломатом розвідувально-підбивної діяльності, окрім можливої належності його до розвідувального апарату іноземної спецслужби. Подібним випадком є і справа *Leander v Sweden*, яка стосувалась проведення таємних перевірок щодо особи, яка претендувала на роботу за договором в установі військового підпорядкування. В інших випадках держави, що надавали пояснення про наявність випадків для обмеження прав і свобод, іноді не розділяли національну і громадську безпеку. Це, наприклад, стосується справи *Malone v United Kingdom*, щодо ведення прослуховування комунікацій особи в межах таємної поліцейської діяльності з протидії організованій злочинній діяльності.

Доволі неоднозначним є сприйняття інтересів національної безпеки, як підстави для обмеження прав, передбачених ст. 11 Конвенції щодо свободи об'єднань. Сучасний політичний контекст обумовлює існування значної судової практики ЄСПЛ у справах стосовно Туреччини та деяких інших країн. Політична ситуація і політичний режим в Туреччині викликає доволі широкі заборони на різноманітну політичну активність, у т. ч. державних заборон щодо деяких ідеологій та діяльності конкретних політичних партій та громадських об'єднань.

Виходячи з їхньої мети створення та існування, сама по собі ідеологія може бути достатньою підставою для прийняття рішень щодо заборони лише в окремих випадках. Практика Європейського Суду з прав людини підтверджує це. Як правило мова йшла про

діяльність політичних партій крайніх поглядів, релігійно-політичних утворень, а також політичних організацій націоналістичного і сепаратистського спрямування.

При цьому позиція Суду з одного боку зумовлює існування конкретних доводів (фактів, дій) для заборони політичної організації (наприклад, справи «*Sidiropoulos and others v Greece*», «*United Communist Party v Turkey*» та інші). Водночас, мають місце рішення коли задекларована мета політичної партії сама по собі вважалась достатньою підставою для заборони її діяльності, оскільки мова йшла про прихильність ідеології «шаріату», або схвалення терористичної діяльності («*Refah Partisi v Turkey*», «*Herri Batasuna et Batasuna v Spain*»).

Але в даному разі судові рішення ухвалювались у політико-правовому контексті і стосувались заборони політичної діяльності або реєстрації. Для України занепокоєння викликає ситуація із заборonoю Комуністичної партії України та низкою пов'язаних із цим проблем. Скоріше за все остаточно правова оцінка зазначеного знайде своє відображення у майбутніх рішеннях Європейського суду з прав людини. Окрім цього, законодавчі новації стосуються і можливих оцінок суті певної ідеології. Мова йде про Закон України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки», що визнаний конституційним рішенням Конституційного Суду України від 16.07.2019. У цьому рішенні наведено доволі ґрунтовний аналіз комуністичної ідеології, а також діяльності Комуністичної партії СРСР та радянських органів державної влади. Занадто значне політичне забарвлення рішення було підкреслено в окремих думках деяких суддів Конституційного Суду щодо цього рішення. Водночас, остаточно питання юридичної оцінки ідеології може бути вирішено скоріш за все на рівні ЄСПЛ у межах розгляду справ, що прямо пов'язані із заборonoю КПУ.

Окрім рішень щодо політичної діяльності та політичних партій питання правової оцінки певної ідеології може виникнути і щодо діяльності окремих груп у сучасному інформаційному суспільстві, оскільки задекларована можливість такої оцінки на рівні вищих судових інстанцій може зумовити доволі широке поле для політико-правової активності держав.

Таким чином, практика застосування Конвенції, а також практика Європейського Суду з прав людини у питанні визначення інтересів національної безпеки, як підстави для обмеження прав людини, що вважається легітимною підставою у міжнародно-правових актах, існує і є доволі повною. Але ця практика уникає чіткого визначення поняття «національна безпека», зосереджуючи насамперед увагу на побудові системи відповідних гарантій дотримання прав. Безумовно, що бурхливий розвиток інформаційних технологій та інші фактори сучасного інформаційного суспільства мають значний вплив на правове регулювання у сфері забезпечення національної безпеки. Водночас загальні правові підходи щодо чіткості законодавчого визначення підстав для обмеження прав і свобод, гарантій від можливих зловживань у цій сфері та ретельного визначення важливості суспільної мети залишаються незмінними. Перспективним у цьому контексті будуть подальші дослідження особливостей впливу факторів інформаційної епохи, у першу чергу прямо викликаних розвитком технологій, на стан дотримання прав і свобод людини у сучасному світі, зокрема особливості формування, трансформації та розповсюдження транснаціональних ідеологій, глобального активізму та модернізованих суб'єктів політики.

Ткачук Т.Ю.

доктор юридичних наук, доцент,
заступник завідувача кафедри організації захисту інформації з обмеженим доступом Навчально-наукового інституту інформаційної безпеки Національної академії СБ України

СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

У найзагальнішому розумінні глобальна інформаційна сфера має дві компоненти, котрі водночас є основними складовими інформаційної безпеки: *технічну* – антропогенне штучне середовище техніки й технологій і *психологічну* – світ природи з його емоціями.

Предмет правового забезпечення інформаційної безпеки людини – це пов'язані з інформаційною сферою суспільні відносини, які виникають у двох її складових: технічній – комп'ютерні системи, телекомунікаційні мережі та інформаційно-психологічній – національні цінності, суспільна думка, індивідуальна та суспільна психологія.

У цьому дослідженні розглянемо детальніше інформаційно-психологічні аспекти. Не зайве підкреслити, що пріоритетному захисту в цьому разі підлягає саме суспільна свідомість українців. Адже сьогодні вже маємо безліч переконливих прикладів, як маніпулювання суспільною свідомістю та інші деструктивні інформаційно-психологічні впливи викликають, провокують або сприяють серйозним дисфункційним суспільно-політичним процесам, котрі можуть призвести до розбалансованості та імпотенції владних структур, соціально-політичних напружень, безладів, потрясінь і т.п.

Як один із окремих фундаментальних елементів системи національної безпеки України інформаційна безпека нерозривно пов'язана з усіма іншими складовими безпеки, успішне функціонування яких значною мірою залежить від рівня її забезпечення. Ми погоджуємося з О.Корейком, що сьогодні інформаційний складник не існує поза межами загальної національної безпеки, так само як і

національна безпека не буде всеосяжною без інформаційної своєї складової [1, с. 9].

Розглянемо докладніше кожен із видів інформаційної безпеки людини. Пріоритетними об'єктами забезпечення *духовної безпеки* є: мова як головна ознака нації, основа національна культура та історичної спадщина народу; наука, освіта, мистецтво, а також головне джерело інформування суспільства – засоби масової комунікації. Інформаційно-психологічне протистояння та пропаганда вважаються найбільш ефективними з-поміж методів захисту духовної сфери.

Основними засобами інформаційно-психологічного впливу є дезінформація й різноманітні методики маніпулювання свідомістю людини й суспільства з метою їх деморалізації й прихованого керування поведінкою. Головним завданням таких впливів є формування у людини й соціуму в цілому спотворених поглядів на навколишній світ і самих себе шляхом пропагування, навіювання фальшивих цінностей, хибних пріоритетів і цілей.

Забезпечення *військової безпеки* визначальною мірою пов'язане сьогодні з упровадженням інформаційних технологій. Відтак, небезпека від ураження сучасних комп'ютеризованих систем управління військом, систем озброєння, логістики тощо кібернетичною зброєю противника, його інформаційними атаками значно підвищується. Недооцінка чи навіть нехтування цих реалій стало одним із найвагоміших чинників трагічних подій на півдні та сході нашої країни.

Економічна безпека як складова інформаційної безпеки людини у системі національної безпеки пов'язана з так званою інформаційною економікою, котра виникла як результат прогресу інформаційних технологій, створення глобальних інформаційно-телекомунікаційних систем, зростання потреб населення в інформаційних послугах. А про визначальний вплив економіки на всі сфери суспільного розвитку, напевно, не варто зайвий раз говорити [2, с. 370].

У теперішній час, як слушно зазначають фахівці, інформаційна безпека національної економіки атрибутивною ознакою суверенітету держави та її цілісності. При цьому стабільний соціально-економічний і політичний прогрес країни на основі сучасних інно-

вацій багато в чому залежить від формування ефективної системи інформаційної безпеки [3, с. 45]. Розвиток інформаційної економіки стає стратегічно важливим чинником сучасної геополітики. Тому актуалізується також потреба унормування таких економічних явищ, як, приміром, криптовалюта, електронна комерція, Інтернет-розрахунки та інших нових суспільних відносин.

Соціальна безпека як складова інформаційної безпеки людини передбачає захист інтересів населення у цій сфері, суспільних відносин, способу життя, функціонування громадських структур, систем життєзабезпечення, адекватних сучасному етапу цивілізаційного розвитку.

Людина й людські спільноти завжди є головним об'єктом усіх форм управління, в тому числі й механізмів інформаційного керування. Сучасні інформаційні технології значно розширили можливості й підвищили ефективність впливу на психіку і свідомість людей, завдяки впровадженню новітніх методів, засобів і прийомів латентного маніпулювання. Відтак, загроза дегуманізації настільки актуалізувалася, що саме життя людини вийшло на передній план у структурі сучасних цінностей. При цьому в контексті державно-правового захисту зазіхання на психіку людей вважаються, як правило, другорядними порівняно з фізичними посяганнями. І якщо правове забезпечення взагалі зазвичай не встигає за процесами суспільного розвою, то про духовну сферу, особливо щодо безпекових проблем, годі й говорити. Тому питання правової захищеності свідомості людей є сьогодні серед головних пріоритетів.

Зловмисне використання інформаційних технологій задля провокування соціального розшарування суспільства шляхом розподілу інформаційного продукту, диссолюції інститутів, спрямованих на розвиток особистості, інспіруванні розколу суспільства на підставі етно-національних, ідеологічних, мовних, конфесійних та інших чинників призводить до негативних деформацій соціальної сфери. Отруйні «плоди» такої інформаційної агресії Російської Федерації вже багато років лихоманять українське суспільство.

Атрибутом інформаційного суспільства є засоби масової інформації, котрі на сьогодні є по суті монополістами на ринку задоволення інформаційних потреб соціуму, як на рівні окремого насе-

леного пункту, регіону, країни, так і у світовому масштабі. Відтак, вони здатні нав'язувати певні ідеологічні погляди й настанови, формувати громадську думку, виступити надпотужним чинником як стабілізації та згуртування суспільства, так і провокування соціальних заворушень і вибухів. З огляду на це в теперішній час усе частіше порушується питання про достовірність та якість інформації, що ретранслюється ЗМІ, посилення відповідальності за це суб'єктів означеної сфери. Звісно, усі спрямовані на це заходи мають здійснюватися виключно у правовому полі, а тому, як бачимо, досягти бажаного рівня соціальної безпеки неможливо без належного правового забезпечення інформаційної безпеки.

Бурхливий розвиток електронних технологій зумовив також виникнення нових серйозних загроз навколишньому природному середовищу, здоров'ю та життю людей, що актуалізувало й глобалізувало питання забезпечення екологічної безпеки. Забруднення повітря, землі та водойм, знищення багатьох видів живих організмів і цілих екосистем, руйнування озонового шару планети, техногенні катастрофи (Чорнобиль, Бхопал, Фукусіма та багато інших), створення й застосування нових видів зброї, – ось далеко не вичерпний перелік наслідків реалізації подібних загроз.

З-поміж основних шляхів розв'язання безпекових проблем у цій сфері – екологічний моніторинг, моделювання природних процесів, обчислення й урахування антропогенних навантажень і техногенних впливів на навколишнє середовище. Упевнені, що продуктивність таких заходів значною мірою залежить від цілеспрямованого застосування новітніх інформаційних технологій. Отже, безпосередній зв'язок екологічної та інформаційної безпеки цілком очевидний.

Таким чином, унікальна специфіка феномену інформаційної безпеки, котра є атрибутивною ознакою всього безпекового спектру – економічної, соціально-політичної, військової та екологічної безпеки, – зумовлює її визначальну роль у процесі забезпечення національної безпеки. Іншими словами, умови та ефективність забезпечення основних видів безпеки людини, суспільства й держави на сучасному етапі розвитку соціуму вирішальною мірою залежать від забезпечення інформаційної безпеки.

Більше того, сьогодні активно дискутується питання про так звану екологію інформації. Показовою з цього приводу є праця Фелікса Сталдера, яка так і називається – «Екологія інформації» [4]. На підставі свого дослідження вчений резюмує, що медіа створюють інтегроване середовище (environment), основу якого становлять потоки інформації. Все частіше в діяльності людини це середовище стає головним. Екологія інформації прагне зрозуміти його властивості, щоб використовувати потенціал цього середовища, уникати небезпек і позитивно впливати на його розвиток.

У цьому контексті ми підтримуємо Р. Проданюка, який зазначає, що інформаційна безпека може розглядатись як одна із соціальних інституцій контролю за підтриманням інформаційної рівноваги, функція якої полягає в підтриманні екологічності інформаційного простору [5, с. 87].

Розвиток інформаційних технологій на початку 21 століття визначив загальні тенденції поступу людства та окреслив характерні проблеми даної епохи, серед яких:

1. Формування нового планетарного простору, в основі якого інформаційні й телекомунікаційні технології забезпечують ефективну взаємодію між людьми. Основними характеристиками таких процесів є безмежність, доступність, гіперпов'язаність, «стирання» територіальних кордонів, рух у масштабі часу, розвиток Інтернету речей тощо. Як наслідок, відбувається становлення нового інформаційного суспільства.

2. Усі без винятку суспільні процеси (політичні, соціальні, економічні) залежать від використання інформаційних технологій, оскільки вони мають вирішальне значення у формуванні існуючої реальності й мають неабиякий вплив на її розвиток.

3. Недостатня увага з боку як міжнародних інституцій, так і національних урядів, до проблем правового забезпечення інформаційної безпеки стали причиною виникнення та надшвидкого поширення понять «інформаційна зброя», «інформаційний тероризм» та «інформаційна війна», а також деструктивних впливів від позначуваних цими термінами явищ. Значне применшення завдань інформаційної безпеки стало причиною непрогнозованих економічних, соціальних, екологічних, політичних та інших потрясінь у

системі безпеки. Унаслідок цього вирішення питань інформаційної безпеки із значним запізненням вийшло на перший план в усіх сферах суспільного життя і державної діяльності, як на національному, так і на міжнародному рівнях.

Як бачимо, у досліджуваній системі можемо виокремити *глобальну безпеку*, позаяк у загальносвітовому контексті інформаційна безпека набуває статусу всеосяжної проблеми сучасного етапу розвитку людства. Вказаний характер глобальної безпеки зумовлює такі її ознаки, як:

- вона охоплює усі без винятку країни світу;
- вона є об'єктивною передумовою і провідним засобом прогресу світової спільноти;
- як перша стадія ноосфери інформаційна безпека вона є актуальним завданням в умовах формування світового інформаційного суспільства;
- нехтування питаннями інформаційної безпеки відкриває шлях інформаційним війнам інформаційному тероризму та іншим загрозам.

Звідси випливає, що для посилення інформаційної безпеки, запобігання негативним інформаційно-психологічним впливам на людину й суспільство та їх припинення потрібні спільні скоординовані зусилля усього міжнародного співтовариства.

Таким чином, виникла потреба створення загальносвітової системи інформаційної безпеки, оскільки в реаліях світового інформаційного простору інформаційна безпека може бути ефективно забезпечена лише спільними діями всіх держав. Система глобальної інформаційної безпеки має стати важливим чинником сталого прогресу у глобальних масштабах. Зрозуміло, що така кооперація – справа складна й потребує тривалої, злагодженої, конструктивної співпраці. Убачається, що подібні перемови доцільно починати на рівні підінститутів, як, скажімо, проект Міжмор'я (Intermarium) та аналогічні.

Питаннями, які мають розглядатися в межах таких міжнародних проектів розвитку глобальної інформаційної безпеки, можуть бути, наприклад, такі:

- захист глобального інформаційного середовища від реальних і потенційних загроз і викликів;

– безпечні для людини, суспільства й навколишнього середовища напрями розвитку інформаційного простору;

– розвиток інформаційної культури людини й суспільства.

При цьому важливо пам'ятати, що захист і зміцнення безпеки світового інформаційного простору, який не визнає географічних і державних кордонів, – спільна справа всього міжнародного співтовариства, позаяк його вразливість і шкода від нього відбивається на всіх без винятку країнах. З огляду на це убачається доцільним висунути на порядок денний питання узгодження національних стандартів і законів, співпраці з їх реалізації, укладання міждержавних угод у соціальній, політичній, культурній, юридичній та інших сферах функціонування міжнародного інформаційного простору.

Література:

1. Корнейко О. Застосування та визначення терміна «інформаційна безпека» в національному законодавстві. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. Науково-технічний збірник, 2009. Вип. 2(19). С. 9-13

2. Drucker P.F. The Age of Discontinuity. Guidelines to Our Changing Society. London: New Brunswick (US), 1994. P. 370

3. Білак Ю.Ю. Інформаційна безпека як елемент підвищення Ефективності інноваційного розвитку України. Вісник КНУТД №4 (113), 2017. С. 44-50

4. Stalder F. Information Ecology; McLuhan Program in Culture and Technology, 1997. URL: <http://felix.openflows.com/html/infoeco.html>

5. Проданюк Р. І. Інформаційна безпека в соціологічному контексті: до постановки проблеми. Науково-теоретичний альманах «Грані». 2018. Т. 21. № 4. С. 84-90

Калиновський Ю.Ю.

доктор філософських наук,
професор, професор кафедри
філософії Національного
юридичного університету
імені Ярослава Мудрого

ЦІННІСНА БЕЗПЕКА ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ

Сучасні інформаційні технології відкрили для людини низку нових можливостей, але в той же час стали підґрунтям для небезпек і загроз її духовно-ціннісному світу. На сьогоднішній день людина, що занурюється у віртуальний простір має бути готова протистояти відкритим та латентним загрозам щодо збереження не тільки її персональних даних, інтелектуальної власності, але й аксіологічних детермінант її буття.

На нашу думку, ціннісна безпека людини у комунікаційно-інформаційному полі є невід'ємною складовою духовної безпеки суспільства й держави. Розмірковуючи про співвідношення безпеки людини, суспільства та держави І. Дуднікова підкреслює, що людина (особистість), будучи сама об'єктом і суб'єктом, системою безпеки, присутня у всіх інших системах безпеки, відіграючи базову системоутворюючу роль. Звідси забезпечення особистої безпеки стає умовою забезпечення безпеки всіх інших її форм і рівнів, але, у свою чергу, становище особистості визначається станом суспільства, держави, природи. Особистість знаходиться у фокусі практично всіх небезпек, оскільки від будь-яких деструктивних соціально-політичних, екологічних, етнічних і технічних подій страждає сама людина. Особиста безпека, захищеність людини від чинників небезпеки на рівні її особистих інтересів і потреб, має безліч різновидів. Це пов'язано з тим, що особистість є біосоціальною системою і виступає одночасно в ролі і людини як члена суспільства, і людини як живого організму, існуючого в обмежених параметрах навколишнього середовища. У першому випадку мова йде про правову безпеку особистості, захищеності людини і

громадянина системою загальнообов'язкових соціальних норм, що охороняються традиціями суспільства і правовою діяльністю держави; про матеріальну безпеку, захищеність її власності, господарських, майнових, трудових і родинних відносин; про побутову безпеку, захищеність споруд і систем життєзабезпечення, житла, інженерно-комунальних мереж та ін. У другому випадку особиста безпека визначається за класом параметрів середовища мешкання особистості: фізична, хімічна, біологічна, радіаційна та інші, а також за характером впливу – соматична, психічна, духовна, фізіологічна, енергетична [1, с. 13-14.].

Безсумнівно ціннісна безпека людини у інформаційному суспільстві не може розглядатися окремо від інших суб'єктів та об'єктів системи загальної безпеки. З точки зору О. Павлишина, основні світоглядні загрози духовно-ціннісній безпеці людини, суспільства та держави (які мають переважно внутрішній характер) є такими:

1) культурно-ціннісна загроза (низький рівень розвитку світогляду, загальної та правової культури кожного члена суспільства, нерозвинене світобачення та світосприйняття особистості, недостатньо сформована система індивідуальних цінностей, відсутність власної життєвої позиції);

2) ідейно-доктринальна загроза (відсутність єдиної державної теоретичної суспільно-ідейної платформи, що призводить до заміщення відповідних прогалів альтернативними ідеологічними концептами);

3) суспільно-організаційна загроза (відсутність світоглядних, а відповідно – правових та організаційних передумов формування політичної свідомості населення та побудови дієвого механізму політико-правового забезпечення суспільного життя, здатного консолідувати суспільство, використати його неоднорідність як таку властивість соціальної системи, що додає їй гнучкості, динамізму, різноманітності, а отже, життєздатності. Наслідком цього є наявність перманентних антагонізмів або відмова від активної участі в політичному житті, байдужість до реалізації людиною своїх прав і обов'язків, які можуть призвести до дезінтеграції українського суспільства) [2, с. 48-49].

На сьогоднішній день, характер та рівень небезпек духовно-ціннісному буттю людини у вітчизняному соціумі обумовлений зокрема й тим, що Україна стала об'єктом інформаційних, "гібридних" війн, методи ведення яких спрямовані у першу чергу на руйнування світогляду людини та суспільства у цілому.

Як стверджують фахівці, Україна на сучасному етапі державотворення стикається з посяганнями не тільки на територіальну цілісність, а й на духовний та інформаційний суверенітет. Загрози духовній сфері нашої країни мають яскраво виражені ознаки гібридності: вони становлять комплексний характер й поєднують інформаційні, комунікаційно-технологічні, пропагандистські та інші заходи. Безумовно, основний негативний вплив на духовність українського народу здійснюється за допомогою засобів масової комунікації. Можна констатувати, що Україна стала як об'єктом, так і суб'єктом інформаційної війни [3, с. 33].

Необхідно зазначити, що в інформаційній сфері права людини, як фундаментальна цінність демократичного суспільства, виявляються найбільш незахищеними з декількох причин: нерозвиненість законодавства щодо захисту прав людини у комунікаційно-інформаційній сфері, стрімке поширення кіберзлочинності, транснаціональний характер "інформаційної" злочинності, низький рівень інформаційної культури користувачів, динамічний розвиток інформаційно-комунікаційних технологій тощо.

Вочевидь, одним з базових чинників забезпечення ціннісної безпеки людини є підвищення рівня її інформаційної культури. Розвинена інформаційна культура в наш час передбачає не тільки здатність знаходити необхідну інформацію, відфільтровувати спам, протистояти негативним інформаційним впливам, не піддаватися маніпулятивним технологіям, а й розуміння сутності загальнолюдських, національних, особистісних цінностей, вміння їх захищати й відтворювати у соціальних та інформаційно-комунікаційних відношеннях.

З точки зору О. Золотар, важливим елементом інформаційної культури є інформаційна стійкість. Україна геополітично ввесь час знаходиться на межі кількох потужних культурних традицій. З одного боку, в Україні, як і в більшості країн Східної Європи

відбувається активне насадження прозахідних цінностей. З іншої сторони має місце загроза російської пропаганди, яка в окремих регіонах вже є реалізованою і наслідком якої є гібридна війна. Безумовно, формування нової системи цінностей і вироблення ідеологічної системи, спрямованої на її підтримку, є складним завданням, яке вимагає ґрунтовного опрацювання і дослідження. Разом з тим, відсутність такої системи шкодить як інформаційній безпеці окремих громадян, так і безпеці держави загалом. Зазначена ситуація ускладнюється тим, що сама держава відвернулася від інформаційного й ідеологічного захисту своїх громадян. Це ще раз підтверджує необхідність спрямування інформаційної культури на формування інформаційного імунітету особистості, забезпечення її інформаційної стійкості [4, с. 231].

Варто зауважити, що рівень загроз інформаційним правам та цінностям людини багато в чому обумовлений ступенем її зануреності у віртуальний та комунікаційний світи. Зокрема, Д. Мехед доводить, що при системному розгляді різних видів порушень захисту конфіденційної інформації в соціальній мережі можна виділити наступні типи основних загроз інформації в соціальній мережі:

- загроза конфіденційності (витік конфіденційної інформації та заподіяння прямого або непрямого збитку користувачеві соціальної мережі);
- загроза цілісності (модифікація інформації у середині мережі втрата її адекватності);
- загроза доступності (порушення доступу до мережевої інформації і блокування доступу до ресурсу);
- загроза повноті (знищення інформації у середині мережі та заподіяння прямого або непрямого збитку як користувачеві соціальної мережі, так і її власнику);
- загроза актуальності (затримка отримання легальним користувачем мережі інформації);
- загроза важливості (несанкціоноване читання конфіденційної мережевої інформації, що призводить до втрати її ціннісних характеристик);
- загроза адресності (переадресація мережевої інформації, що може призводити до зниження її конфіденційності та доступності);

– загроза надмірності інформації (багаторазове дублювання мережевої інформації) [5, с. 17].

В той же час, в умовах перманентного прогресу інформаційних технологій варто не забувати про забезпечення ціннісної безпеки людини. Так, прагнучи увійти до Європейського Союзу, українська держава має послідовно захищати системоутворюючі, демократичні цінності найважливішою з яких є права та свободи людини. Динамічний розвиток інформаційного суспільства потребує особливої уваги до збереження й відтворення класичних демократичних цінностей, їх репрезентації й захисту у комунікаційно-інформаційному просторі.

Як відомо, головні демократичні цінності містяться в Хартії фундаментальних прав Європейського Союзу. Згідно з означеним документом до базових європейських цінностей належать:

- гідність – основний орієнтир у європейській моделі захисту прав людини. Саме із забезпечення поваги до гідності людини починається реалізація і захист її прав та основоположних свобод;

- права людини – невід’ємні та обов’язкові для дотримання всіма громадянами політичні, економічні, соціальні, культурні та інші можливості життєдіяльності, надані людині від природи, без яких вона не може повноцінно існувати як людська істота;

- свобода особистості – одна з істотних ознак людського буття, що становить необхідну умову існування суспільства, виявляє вищу духовну суть людини і цінність її життя;

- рівноправність – рівність усіх громадян суспільства перед законом і судом, наявність рівних конституційних прав і свобод;

- солідарність – однаковість, спільність інтересів; соціальна згуртованість, єдність дій, спільна діяльність, у процесі якої досягаються певні цілі, розв’язуються суспільні проблеми, реалізуються спільні інтереси;

- законність, вираженням якої є правова держава, що являє собою політичну організацію, затверджену народом на основі принципу розподілу влади й уповноважена забезпечувати його суверенітет, національні інтереси та національну безпеку на основі принципу справедливості та захисту прав і свобод особи і громадянина;

– демократія– влада народу, що виходить з організації та функціонування державної влади на засадах визнання народу її джерелом і носієм, ґрунтується на прагненні забезпечити справедливість, рівність і добробут усіх при розв’язанні проблем і питань суспільного врядування;

– громадянськість – це спрямованість на об’єднання з іншими людьми задля захисту своїх інтересів, прав і свобод, завдяки чому суспільство стає громадянським, а індивід – громадянином [6, с. 19].

Загалом, для забезпечення аксіологічної безпеки людини, необхідно визначити базові цінності, довкола яких згрупуються інші цінності та ідеї, утворюючи безпечні умови для існування людини та суспільства в цілому. Відповідна новітня система цінностей має бути спрямована на об’єднання суспільств та людей, на забезпечення гідних та безпечних умов життя особистості в сучасному суспільстві. Зрозуміло, що аналіз ціннісних основ безпеки людини є основою для формулювання політики регулювання ціннісної системи українського суспільства, насамперед через політичну дію громадян та суспільних груп. Синтез процесів соціокультурної та національної самоідентифікації українського народу, що здійснюється у ході будівництва незалежної держави, означає реалізацію специфічного соціокультурного проекту, складовими якого слід вважати в першу чергу відродження культурної історичної пам’яті, рефлексію всього без винятку попереднього культурно-історичного досвіду та його реконструкцію на основі нової системи цінностей та орієнтації [7, с. 32].

Отже, ціннісна безпека людини в інформаційному суспільстві набуває особливої значущості в умовах глобальних й локальних протистоянь, у яких інформація, цінності та знання є не тільки духовними феноменами, а й потужною зброєю. У даному контексті захист вітчизняного інформаційно-культурного поля від зовнішніх втручань постає одним з стратегічних завдань українського державотворення.

Список використаної літератури

1. Дуднікова І. І. Безпека життєдіяльності / І. І. Дуднікова. – Київ: Вид-во Європ. ун-ту, 2003. – 268 с.

2. Павлишин О. В. Семіотико-правовий аналіз основних загроз духовній безпеці суспільства та передумов їх подолання в сучасній Україні / О.В. Павлишин// Духовна безпека України: погляд суспільствознавства і богослов'я: матеріали XVII науково-практичної конференції (м. Київ, 17 травня 2018 р.). – Київ: ВНЗ «Національна академія управління», 2018. – С. 47-49.

3. Мануйлов Є. М. Духовні імперативи вітчизняного державотворення: аксіологічний та безпековий контексти / Є.М. Мануйлов, Ю.Ю. Калиновський //Вісник Національного юридичного університету імені Ярослава Мудрого. Серія: Філософія / редкол. : А. П. Гетьман та ін.– Харків: Право, 2020. – № 1 (44). – С. 23-38.

4. Золотар О. О. Інформаційна безпека людини: теорія і практика: монографія / О. О. Золотар. – Київ : ТОВ «Видавничий дім «АртЕк», 2018 – 446 с.

5. Мехед Д. Інформаційна безпека в соціальних мережах. Методи поширення інформації в соціальних мережах / Д. Мехед //Прав., нормат. та метрол. забезп. системи захисту інформації в Україні: наук.-техн. зб. – 2015. – Вип. 2. – С. 14-18.

6. Мадрига Т. Б. Європейські цінності та ціннісні орієнтації українського суспільства: проблеми співвідношення / Т. Б. Мадрига // Прикарпатський вісник НТШ. Думка. – 2015. – № 3. – С. 96-103.

7. Калиновський Ю. Ю. Аксіологічна безпека особистості в умовах інформаційної війни / Ю. Ю. Калиновський, О. О. Павліченко // Науково-практична конференція Харківського національного університету Повітряних Сил імені Івана Кожедуба «Сучасна війна: гуманітарний аспект», 31 травня-1 червня 2018 р. – Х.: ХНУПС ім. І. Кожедуба, 2018. – С. 31-33.

Батиргарєєва В.С.

доктор юридичних наук, старший науковий співробітник,
головний науковий співробітник
Науково-дослідного інституту інформатики і права Національної академії правових наук України,
директор Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса Національної академії правових наук України

**ІНФОРМАЦІЙНИЙ ПРОСТІР ЯК ПРОВОКУЮЧИЙ
ЧИННИК У ДЕТЕРМІНАЦІЇ ВЧИНЕННЯ ЗЛОЧИНІВ**

Вже сьогодні з усією відповідальністю треба констатувати, що жодний регіон або країна світу навіть жодна людина (за дуже незначним виключенням) не сприймаються як замкнуті, самодостатні системи, оскільки людство перебуває на порозі глобального перебалансування свого соціального довкілля, що несе як очевидні блага, так і значні ризики. І так сталося, що *Homo Criminalibus* один із перших оперативно реагує на ті можливості, які відкриває перед людиною глобалізація світу, особливо у секторі, пов'язаному із використанням досягнень сучасних інформаційних технологій. Напевно, надалі залишатиметься небагато злочинів, яких неможливо було б вчинити у режимі online або ж принаймні без використання інших досягнень так званого шостого рівня техніко-економічної парадигми, або технологічного укладу світу, із дистантними формами людської взаємодії. Зараз, наприклад, не є «проблемою» придбати наркотичні засоби або довести людину до самогубства за допомогою Інтернету. Стає можливим навіть вчинити хуліганство у такий самий спосіб, не говорячи вже про «класичні» випадки кібершахрайства. Отже, нескладно здогадатися, що будь-хто з нас є потенційною жертвою правопорушень в інформаційному просторі, оскільки, кіберкримінал, що нерідко до того ж набуває організованих рис (особливо в умовах пандемій та інфоде-

мій), безсумнівно, згодом намагатиметься збільшувати прибутки від вчинення кібершахрайств, фінансових злочинів, реалізації контрафактних і нелегальних товарів, поширення дезінформації та розквіту онлайн-індустрій (порнографія, незаконні казино та ін.) у режимі online та скоєння інших видів злочинів. Відомості, одержувані з різних країн світу – з Китаю, США, Норвегії, Індії, Італії та Японії, – свідчать про те, що кіберкримінал, на відміну від традиційних видів організованих злочинних угруповань, стрімко зреагував на пандемію і використовує можливості, що відкрилися [1].

Водночас, коли глобалізуються політичні, економічні, культурні, інформаційні процеси, все більше і більше стирається й таке поняття, як національна злочинність, на зміну якої приходять її транснаціональні форми з «міжнародним елементом». Тому недаремно, що явище глобалізації злочинності ставиться в один ряд із проблемами глобальної зміни клімату, відсталості країн третього світу та масового голоду, поширення зброї масового ураження та ядерної катастрофи. Таким чином, процеси глобалізації «змушують» злочинність набувати, так би мовити, наддержавні риси та розвиватися за ще невивченими законами її буття.

Крім того, сьогодні ми є свідками того, що поряд із традиційними проявами злочинності, народжуються зовсім нові її прояви (якраз з використанням можливостей інформаційного простору). Адже будь-яке лихо планетарного масштабу, до речі, яке ми всі зараз відчуваємо у зв'язку із поширенням коронавірусу, дає небувалий поштовх для кримінальної активності. Так, наприклад, породженням глобалізації світу є масове поширення дезінформації із приводу ключових проблем, що турбують людство. Одним із наслідків її поширення є інфодемія, яка, у свою чергу, виявляється живлячим ґрунтом для криміналітету. Поширення фейків, підняття градусу панічних настроїв, урешті-решт, загрожує продукуванням, з одного боку, небезпечної віктимної, а з другого боку, протиправної поведінки людей. Якщо вся увага людини в періоди масової інфодемічної істерії прикута до інформаційної сфери, то злочинці все частіше і частіше вдаються до вчинення протиправних діянь із використанням саме кіберпростору. До того ж це в значній мірі «убезпечує» їх злочину діяльність від викриття, а значить, зайвий

раз виступає провокуючим чинником у детермінації протиправної поведінки.

У березні 2020 р. Європол опублікував доповідь під назвою «Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis» («Пандемічний спекулянт: як злочинці експлуатують кризу COVID-19»), в якій стисло викладено позицію аналітиків Європолу щодо головних змін у кримінальній дійсності пандемічного періоду. Так, відмічається, що правопорушники швидко скористалися можливостями, які відкриває криза, адаптуючи до цього свою злочинну діяльність або вдаючись до вчинення нових злочинних дій. Серед чинників, що впливають на відмічені зміни, зокрема, вказується на залишення громадян дома та дистанційний характер роботи з використанням можливостей Інтернет-простору, непомітність деяких кримінальних дій та їх перенесення на онлайн-пристрої внаслідок обмежень у суспільному житті; скорочення поставок певних незаконних товарів до ЄС тощо [2]. При цьому, ґрунтуючись на інформації, наданої державами-членами ЄС та власними експертами, Європолом робиться висновок про зростання кіберзлочинності та формування нового, так званого карантинного типу організованої злочинності, коли групи правопорушників реалізують цілі схеми, видаючи себе за представників органів влади та медиків із метою вчинення шахрайства і крадіжок [2].

Все частіше інформаційний простір (зокрема, Інтернет-простір як такий, різного роду соціальні мережі та месенджери) стає майданчиком для висловлювань думок з того чи іншого приводу, що в реальному часі виявляються таким собі ідеологічним підґрунтям для злочинів ненависті (hatecrimes) – насильства та інших протиправних діянь, яким передують знецінення, дегуманізація або профанація певних соціальних груп за ознаками національності, релігії, раси, статі, мови, фізичних ознак [3]. Наприклад, в умовах карантинно-обмежувальних заходів мешканці Ухані зазнають нападів із боку інших китайців і звинувачуються в спалаху COVID-19, а в світових масштабах китайці з тих пір піддаються міжнародній стигматизації [4]. Свого часу спалах лихоманки Ебола в 2014 році, що вважалася проблемою африканського походження, призвів до дискримінації осіб африканського походження [5]. І таких прикла-

дів чимало. Не останню роль у детермінації злочинної поведінки відіграє саме інформаційний простір, який здатний в геометричній прогресії за нетривалий час поширювати небезпечний для соціального організму вірус ненависті.

Ще один «темний бік» процесу глобальної інформатизації – можливість здійснення комунікації у підпільній та протиправній діяльності за допомогою DarkNet, що представляє собою інструмент-комунікатор у вигляді прихованої Інтернет-мережі, в якій відбувається з'єднання тільки між довіреними особами, що іноді іменуються як «друзі», з використанням нестандартних протоколів і портів для, зокрема, доступу до заборонених послуг, товарів, вчинення актів тероризму, злочинів у сфері інформаційних технологій, кіберрозвідки тощо [6]. Так, можна навести приклад із сумно звісним сайтом DarkNet під назвою SilkRoad (Шовковий шлях). SilkRoad – сайт для купівлі та продажу наркотичних речовин в розважальних цілях «для тих, кому хочеться час від часу розслабитися у нелегальний спосіб» [7].

Нарешті, людство вже найближчим часом зіштовхнеться з посиленням системи контролю у вигляді цифрового тоталітаризму. Якщо раніше із боку монополістів сотового зв'язку та торгових площадок нав'язувався м'який варіант контролю шляхом обробки персональних даних із метою отримання нібито персоналізованих пропозицій, що обіцяють всілякі бонуси, то далі відбуватиметься жорсткий варіант тотального збору даних і стеження за користувачами таких послуг, під який підводитиметься вельми вагомий аргумент: «безпека важливіше за приватність». Парадигма під назвою «Безпечний світ» лише підштовхне до використання злочинцями тих можливостей, що дає сьогодні суспільству діджиталізація. Отже, повторимося, будь-яка особа а пріорістає віктимною, а знищить, й уразливою від правопорушень в інформаційному просторі.

Фактично інформатизація суспільства створила нову реальність, в якій, на жаль, проблема протидії глобалізованій злочинності звучить все гучніше. Тому завдання учених – гуманітаріїв і представників технічних наук – озброїти людей необхідними знаннями, як протистояти глобалізаційним проявам злочинності в інформаційній сфері. Годі чекати – завтра вже настало!

Використана література:

1. Овчинский В. Преступность COVID – 19: как меняется криминал в период пандемии. URL: zavtra.ru/blogs/authors/5 (дата звернення: 01.06.2020).
2. Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis. URL: <https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis> (дата звернення: 01.06.2020).
3. Злочини на ґрунті ненависті. URL: https://uk.wikipedia.org/wiki/Злочини_на_ґрунті_ненависті (дата звернення: 01.06.2020).
4. Ren, S.-Y., Gao, R.-D. & Chen, Y.-L. (2020). Fear can be more harmful than the severe acute respiratory syndrome coronavirus 2 in controlling the coronavirus disease 2019 epidemic. World Journal of Clinical Cases, Feb 26; 8 (4): 652–657.
5. Monson, S. (2017). Ebola as African: American media discourses of panic and otherization. AfricaToday, 63 (3), 3–27.
6. Даркнет. URL: <https://ru.wikipedia.org/wiki/Даркнет> (дата звернення: 01.06.2020).
7. На темной стороне интернета: Что такое DarkWeb и DeepWeb? URL: https://www.dgl.ru/articles/na-temnoy-storone-interneta-cto-takoe-dark-web-i-deep-web_11677.html (дата звернення: 01.06.2020).

Радзієвська О.Г.

кандидат юридичних наук, провідний науковий співробітник НДІ інформатики і права НАПрН України

НАЦІОНАЛЬНИЙ НАРАТИВ В УМОВАХ ПРОВЕДЕННЯ ІНФОРМАЦІЙНИХ ТА ПСИХОЛОГІЧНИХ ОПЕРАЦІЙ

Основа подальшого розвитку права за Д. Ллойдом закладена в самому праві «відповідно до системи цінностей, що існує у суспільстві» [1, с. 127]. В інформаційному суспільстві, де основними цінностями виступають інформація і знання, а суспільні відносини пов'язані, перш за все, з інформацією, її оборотом, інформаційними продуктами й технологіями, тобто предметом відносин є переважно нематеріальні активи, забезпечення моральності права та відповідності його норм духовним і моральним цінностям суспільства є надзвичайно важливим. Відтак, розвиток системи правового забезпечення гарантованих прав, свобод і безпеки людини в інформаційній сфері та необхідних інститутів для їх реалізації у більшій мірі буде залежним від домінуючої ціннісної парадигми суспільства. Тоді як для ефективного правового регулювання суспільних відносин в інформаційному суспільстві неможливо досягти без детального дослідження чинників впливу на нормативно-ціннісні орієнтири сучасного етапу розвитку цивілізації.

Праворозуміння, а відтак і його складові правотворення та правореалізація, ґрунтуються на духовних цінностях, які є важливою складовою будь-якої культури. Для успішного перетворення існуючої системи забезпечення прав, свобод і безпеки людини в інформаційній сфері у реально діючу бажану систему, узгоджену з міжнародними правовими нормами, необхідно роздивлятися усі нововведення, у тому числі нормативно-правові, через призму духовних та моральних цінностей притаманних окресленому соціальному середовищу. Сприйняття чи відторгнення правових норм, їх ефективність та дієвість залежить перш за все від фундаментальних цінностей, що домінують у суспільстві. Підміна цінностей через корегування національного та геополітичного наративів у

результаті успішно проведених інформаційних та психологічних операцій може загрожувати основним правам, свободам та безпеці громадян по всьому світу.

Наративність є невід'ємною складовою людства, модератором оточуючого світу та засобом його осмислення. Саме наративність є системостворчим елементом самого суспільства, людини та впорядкованості навколишнього світу. Привнесення наративу допомагає узгодити та стабілізувати будь-яку соціальну систему, а його відсутність, або невизначеність – створює хаос в індивідуальному і суспільному світосприйнятті та дезорієнтацію у суспільстві. В епоху глобалізації та інформаційного протистояння роль наративу стає надзвичайно актуальною. Ціллю проведення сучасних інформаційних та психологічних операцій все частіше стає наратив, а метою – його зміна, або підміна. Штучно змінений, або підмінений наратив відкриває можливості для подальшого маніпулювання цим суспільством методом інформаційно-психологічного впливу для отримання переваги в інформаційному протистоянні.

На сьогодні людство виділило три рівні наративів: геополітичний, національний та наратив з питань політики. Геополітичний рівень наративності іноді називають системним, оскільки від відображає системне бачення та основоположні формуючі цінності всього світу загалом. Національний рівень наративності або наратив ідентичності є основою національної самоідентичності та державотворення. Залежно від рівня наративу визначається його модель реалізації та ступінь впливу. Нині на кожному із зазначених рівнів спостерігається загроза трансформації основних наративів у сторону їх викривлення чи підміни через велику кількість цілеспрямованих інформаційних та психологічних атак в рамках сучасних реалій світового інформаційного протиборства та інтенсивного проведення інформаційних війн.

Ще на початку 20-го століття Е. Бернейс, вивчаючи методи управління громадською думкою та технології маніпулювання суспільною свідомістю, дійшов висновку, що важливу роль у маніпулюванні суспільною думкою є групова прив'язаність та суттєва інерційність встановлених звичок і традицій [2].

Зазвичай трансформація цінностей у суспільстві потребувала значного проміжку часу. Вважалося, що ціннісні орієнтири суспільства формуються не одне покоління і не можуть бути зміненими маніпулятивним шляхом. Проте через масовість комунікацій за посередництва нових технологій та інструментів, світової глобалізації й збільшення інтенсивності та ефективності проведення спеціальних інформаційних і психологічних операцій, швидкість трансформаційних процесів у питаннях формування та зміни наративів значно збільшилась, а корегування наративу вже може відбуватися в межах одного покоління. Однак навіть нині швидко змінити думку суспільства на бажану – це надзвичайно складне завдання і потребує системи багаторівневих операцій із застосуванням методів маніпулювання суспільною свідомістю.

Використання багаторівневих довготермінових емоційно забарвлених інформаційних впливів направлених на масову свідомість з «розмитим» закінченням раніше вважалися характерними рисами пропаганди. Інформаційні та психологічні операції визначалися діаметрально протилежними характеристиками. Однак, трансформація цілей, засобів та методів ведення операцій в інформаційній сфері надала їм інших характеристичних властивостей, тим самим замаскувавши їх під пропаганду. Це ускладнило процес виявлення, аналізу та нейтралізації довготривалих, суспільно небезпечних інформаційних загроз.

Серед основних чинників, які створюють можливість для ефективного проведення інформаційних та психологічних операцій слід відзначити недосконалість системи формування запиту на інформацію, а також широке використання систем з елементами штучного інтелекту, зокрема інтернет-ботів, під час комунікації користувачів. Система «запит-відповідь» у мережі технологічно налаштована так, що на запит інформації отримується найбільш популярна відповідь, яка може бути згенерована штучно, а відповіді не верифікуються і не модеруються. Значна частина інформації у мережі цілеспрямовано продукується інтернет-ботами, тобто створена автономними програмами, здатними виконувати прості одноманітні завдання в рамках багаторівневої системи інформаційного впливу. Інтернет-боти стають сьогодні суттєвим інстру-

ментом впливу на формування політичної думки, культури, цінностей та основою для трансформацій у політико-правовій системі держави, однак все ще залишаються поза її нормативно-правовою базою та системним моніторингом. Зважаючи на збільшення кількості інтернет-ботів та надзвичайну популярність сучасних інформаційних платформ соціальні медіа здатні формувати нові суспільні наративи надзвичайно швидко і масово.

Георгій Почепцов [3, с. 143-151] вважає, що втрата наративності нині також можлива через широке використання інформаційно-комунікаційних систем та засобів зберігання (архівування) інформації. При механічній систематизації знань та цифровій обробці інформації втрачаються деякі елементи, які для архівації є несуттєвими, однак були зв'язуючими компонентами безперервності між наративами. Втрата таких складових елементів створює міжнاراتивні пустоти, які згодом індивідуальна або суспільна свідомість вимушена вибудовувати самостійно, опираючись на власну логіку. Саме вказані пустоту легко заповнюються новими наративами з метою підміни понять, цінностей для подальшого управління індивідуальною і суспільною свідомістю. Крім того при цифровізації процесу обробки інформації неминуче накопичуються помилки та неточності, що може призвести до часткової чи повної втрати початкового змісту та ідеї. З точки зору інформаційної безпеки такий вакуумний простір між змістовним наповненням історичного дискурсу, породжений використанням нових інформаційних технологій, створює можливості для маніпулювання індивідуальною та суспільною свідомістю у майбутньому, у тому числі через проведення спеціальних інформаційних або психологічних операцій.

В умовах глобальної соціальної ізоляції, що виникла через запровадження карантинних заходів задля запобігання поширенню вірусу COVID-19, маніпулювання суспільною свідомістю, через вплив на індивідуальну свідомість, у тому числі через підміну наративу, значно збільшилося. Знаходячись у соціальній ізоляції, людина стає ще більш вразливішою в інформаційній сфері. Відсутність прямої комунікації тет-а-тет, переводить особу у симплексний (односторонній) режим споживання інформації та практично позбавляє дуплексної інформаційної взаємодії. Позбавлена

соціального діалогу вона практично узалежнюється від засобів комунікації, особливо від соціальних медіа та мереж. Це єдине місце, де людина може відреагувати на інформацію, висловити свої думки та погляди. Збільшення присутності населення в мережевих спільнотах створює можливості для інфікування інформаційного простору багаторазово тиражованою недостовірною та перекрученою інформацією, фейковими новинами та чутками. Створена фейкова новина швидко поширюється в глобальному інформаційному просторі, створюючи будь-яку потрібну емоцію: чи то страх, невдоволення, гнів, паніку, чи навпаки задоволення, ейфорію, радість. Емоціями соціально ізольованих людей управляти значно легше, а сучасні інформаційно-комунікаційні технології дозволяють зробити це на високому технологічному рівні та великих масштабах. З іншої сторони – недостатність інформації призводить до культивування вимислів і припущень в мережевому соціальному інформаційному просторі, що знову ж таки породжує певні почуття у населення, якими з легкістю можна управляти. Намагання впровадження нових змістів через масове поширення фейкової інформації у суспільну свідомість населення окремих груп чи держав загалом все частіше фіксують фахівці з інформаційної та кібербезпеки. Подібні технології управління масовою свідомістю вивчалися науковцями ще на початку 20-го століття. Відомий вчений, засновник Public Relations (PR) Едвард Бернейс назвав цей метод «інженерією згоди» та вивів на цей рахунок власну теорію, основуючись на дослідженнях відомого психолога Зигмунда Фрейда та власному практичному досвіді успішних рекламних компаній. Вперше напрацювання Е. Бернейса для управління суспільної свідомістю на державному рівні були використані у роботі Комітету суспільної інформації США (Комітет Кріла) у 1913-1919 роках для пропаганди під час Першої світової війни, а згодом у роботі Управління військової інформації США, створеного в 1942 році. Використання інженерії та соціального конструювання як нового підходу, на думку Е. Бернейса, є ефективним засобом створення позитивного або негативного сприйняття запропонованої ідеї, програми, змісту, персони, явища, тощо у будь-якій сфері суспільного життя через налагодження згоди в оцінці цього суспільною думкою. Як і

сто років тому інформаційні і психологічні операції є невід'ємною складовою внутрішнього та міжнародного протиборства за думки та вподобання людей. Зміна масштабів, інструментів та можливостей сучасного світу посилює ефективність їх проведення, а відповідно і ступінь нанесення шкоди.

Перекручування фактів, творення альтернативної історії та її переосмислення призводить до корегування сьогоденних наративів, що дозволить формувати майбутнє окремих регіонів і світу в цілому. Бо наратив – це, в першу чергу, історія (оповідання), яка формує уявлення про світ, про норми, про відхилення від норми, а також визначає маркери «свій-чужий». Впровадження нового наративу в суспільну свідомість може нести реальну загрозу для інформаційної та національної безпеки. Тому надзвичайно важливим завданням нині є виявлення і протидія чинникам, які здатні призводити до трансформації наративів у небажаному, негативно-му напрямку.

Використані джерела

1. Ллойд Деннис. Идея права / Деннис Ллойд; пер. с англ. М.А. Юмашева, науч. ред. Ю.М. Юмашев. – Изд. 3-е. – М.: «КНИГОДЕЛ», 2006. – 416 с.
2. Bernays Edward L. 1928. Manipulating Public Opinion: The Why and The How. – American Journal of Sociology, vol. 33, issue 6.
3. Почепцов Г.Г. Пропаганда 2.0 / Георгий Почепцов; худож.-оформитель М.С. Мендор. – Харьков: Фолио, 2018. – 796 с.

Гаврильців М.Т.

кандидат юридичних наук, доцент
доцент кафедри адміністративно-
правових дисциплін Львівського
державного університету внутріш-
ніх справ

ВИКЛИКИ ТА ЗАГРОЗИ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ В УМОВАХ ГІБРИДНОЇ ВІЙНИ ТА НАПРЯМИ УДОСКОНАЛЕННЯ ЗАСАД ФУНКЦІОНУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційна безпека виступає як невід’ємна складова сучасної системи національної безпеки в цілому і як суттєвий чинник формування громадянського суспільства. Інформаційна безпека – це суспільні відносини, що виникають у процесі організації підтримки, охорони та захисту необхідних для людини, суспільства і держави безпечних умов життєдіяльності, що пов’язані з організацією технологій створення, розповсюдження, зберігання та використання інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави.

Чітке розуміння і виокремлення факторів, що зумовлюють загострення загроз інформаційній безпеці, мають системний характер, а тому вони охоплюють усі без винятку сфери життєдіяльності людини, суспільства і держави. На практиці аналіз викликів – це завжди суб’єктивний процес сприйняття суб’єктом певних факторів через призму власних інтересів і професійності.

Складна політична ситуація, в якій знаходиться Україна останні роки, постійне погіршення іміджу держави на міжнародній арені обумовлені низкою чинників, серед яких важливим фактором є неналежний стан системи інформаційної безпеки. Дехто з фахівців навіть вважає, що в Україні фактично відсутня ефективна система інформаційної безпеки, яка б могла забезпечити виявлення, аналіз інформаційних загроз національній безпеці, а також протидію цим загрозам. Забезпечення інформаційної безпеки сьогодні стає все більш значущою складовою національної безпеки України.

Фахівці називають важливий компонент гібридної війни – вторгнення в інформаційно-комунікаційний простір певної країни з метою придушення опору та формування світового політичного стандарту, узгодженого з інтересами агресора. Для цього використовуються найрізноманітніші інструменти маніпулювання громадською думкою: втручанням у функціонування інформаційно-телекомунікаційних систем та мереж; розвиток кіберзлочинності; вплив на засоби масової комунікації та маніпуляція суспільною думкою [1, с. 18].

Як справедливо зауважує М. Дмитренко, «характер та особливості ведення російсько-української війни свідчать, що її метою є зміна самоідентифікації населення і перетворення східного регіону нашої держави на «сіру зону», яка залишить РФ важелі свого впливу через постійну загрозу поширення нестабільності на всю Україну. Це війна не за території, а за світогляд, думки і душі людей. А оскільки контроль над інформаційною інфраструктурою дає підстави для формування суспільної думки, яка завжди спочатку виявляється в певних переконаннях, а вже потім у конкретних діях то в умовах конкурентної боротьби контроль над інформаційною сферою перетворюється на один із основних ресурсів влади» [2, с. 40-41].

Нині основними визначальними факторами, що негативно впливають на інформаційний простір в Україні, деякі дослідники вважають:

1) постійні втрати серед особового складу (загиблі, полонені, поранені), які ведуть до формування недовіри до українського воєнно-політичного керівництва, що нібито нездатне контролювати ситуацію, що склалася в Україні;

2) недосконала національна система інформаційної безпеки сприяє зниженню рівня патріотизму;

3) активність зовнішніх інформаційних заходів з боку Росії впливає на формування основного твердження про прийнятність для України федерального державного устрою та завершення бойових дій на Сході країни на умовах кремлівського режиму [3, с. 39].

Нова редакція Доктрини інформаційної безпеки України 2017 року актуальними загрозами національним інтересам та націо-

нальній безпеці України в інформаційній сфері визначила: здійснення спеціальних інформаційних операцій, спрямованих на підлив 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, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда федералізму та сепаратизму в Україні [4].

Стратегія національної безпеки України актуальними загрозами національній безпеці України в інформаційній сфері визначає ведення інформаційної війни проти України та відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства [5, с. 12].

Не менш гостро в умовах гібридної війни постає питання кібербезпеки. В сучасному світі кібернетичний простір все частіше слугує для проведення широкого спектра підливних операцій: від викрадення цінної інформації до актів кібертероризму. Насамперед слід зауважити, що усі інформаційні мережі та інформаційні системи містять конфіденційні дані та цінну інформацію комерційного характеру, що підвищує загрозу різноманітних хакерських атак, які можуть мати серйозні у наслідки навіть у національному

масштабі (зокрема, перебої у роботі комунікаційних систем, витік конфіденційної інформації тощо).

Проаналізувавши міжнародні критерії інформаційної безпеки Ю. Нестеряк, виокремив два основні підходи до дослідження цих критеріїв. У рамках першого підходу інформаційна війна розуміється як протиборство інформаційно-комунікаційних технологій та здатності державних і комерційних інформаційних систем забезпечити безпеку інфраструктури держави в цілому. Вчений виокремив такі міжнародні критерії протидії інформаційній агресії:

- 1) захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;
- 2) забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;
- 3) забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні.

Другий підхід виходить через вплив інформації на масову свідомість, маніпулятивний потенціал і психологічний вплив інформаційних повідомлень. До міжнародних критеріїв інформаційної безпеки, зокрема, належить:

- 1) захист власної інформації та інформаційних систем;
- 2) протидія негативному впливу на людську свідомість за допомогою системи засобів масової комунікації;
- 3) захист інформаційних ресурсів і знань людей про самих себе та навколишній світ;
- 4) протидія пропагандистським та психологічним кампаніям, підривним акціям у галузі культури і політики [6, с. 44-45].

Зрозуміло, що сьогодні українське суспільство перебуває під постійною загрозою отримання недостовірної, а подеколи – шкідливої інформації, її несвоечасного надходження, шпигунства, комп'ютерної злочинності тощо. Ці фактори є елементами гібридної війни, що сприяють вторгненню агресора в національну свідомість громадян, підриву національної та інформаційної безпеки.

Основними складовими елементами інформаційної безпеки є як забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, так і захист від негативних інформаційних впливів, що у сукупності мають сприяти цілісності суспільства.

Відтак, першочерговим завданням соціальних і державних інститутів має бути розробка термінових ефективних заходів щодо нейтралізації інформаційно-диверсійної діяльності РФ проти України та запобігання її подальшому розгортанню. Вирішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації.

В умовах гібридної війни держава, що стала об'єктом агресії, неминуче наражається на широкий спектр інформаційних загроз, нейтралізація яких, з одного боку, вимагає вжиття надзвичайних правових і адміністративних заходів, а з іншого – може супроводжуватись істотним згортанням демократичних прав і свобод. Пошук балансу між інтересами національної безпеки та ідеями верховенства права – це стратегічно важливе завдання держави.

Мас-медіа є чи не найфактивнішою зброєю, яка використовується в сучасних гібридних війнах. Зважаючи на це, державна політика в галузі інформаційного права має орієнтуватися на вибіркове застосування обмежень щодо конкретних ЗМІ, які зарекомендували себе недружніми, заангажованими та маніпулятивними. Такий підхід вимагає максимальної правової визначеності обмежувальних критеріїв, оскільки за їх відсутності існує ризик потрапляння під заборону незаангажованих і політично нейтральних мас-медіа (наприклад, у разі нецілеспрямованого поширення недостовірної інформації). Водночас широке коло громадських діячів та організацій наголошують, що встановлені заборони позбавлені фактичних підстав, не мають правового обґрунтування, суперечать Конституції, утискають демократичні права і свободи. Тому, будь-які обмеження в інформаційному середовищі мають носити точковий характер і стосуватися лише тих ресурсів, які скомпрометували себе конкретними діями або є джерелом загроз для держави та суспільства.

Також Україні варто ініціювати міжнародні переговори з проблем забезпечення безпеки в інформаційній сфері. Зокрема, повинні бути досягнуті угоди між максимальною кількістю країн з координації діяльності у сфері боротьби з інформаційним тероризмом, із запобігання цих загроз і узгодження дій та в мінімі-

зації їх наслідків. Предметом переговорів повинен також стати міжнародно-правовий захист національних інформаційних ресурсів та інтелектуальної власності, а також авторських прав на матеріали, поширювані світовими відкритими мережами, в першу чергу через Інтернет. Повинні бути вироблені узгоджені національні та міжнародні правові норми, що встановлюють відповідальність за хакерство та інші комп'ютерні злочини, зловмисне проникнення в державні та корпоративні інформаційні мережі, порушення прав і законних інтересів громадян у процесі інформаційного обміну. Необхідно розглянути можливості контролю за поширенням у мережі Інтернет непристойної і такої, що наносить шкоду суспільній моралі, інформації, недобросовісну рекламу, розпалювання війни, шахрайські операції тощо, які чинять негативний вплив на масову свідомість, фізичне, психічне і соціальне здоров'я людей.

Сьогодні національна інформаційна політика України повинна бути чітко спрямована на забезпечення належних правових, економічних, внутрішньо- і зовнішньополітичних, організаційних та інших необхідних умов, що вкрай важливі для досягнення таких цілей:

- створення розвиненої та захищеної інформаційної інфраструктури України;
- розвитку міжнародного співробітництва в інформаційній сфері та утвердження України як держави стабільного інформаційного суспільства;
- забезпечення інформаційної безпеки життєво важливих інтересів людини, суспільства та держави.

В умовах проведення країною-агресором РФ деструктивного інформаційного впливу на цільову аудиторію України та інших держав світу можна визначити такі основні напрями вжиття заходів щодо захисту національного інформаційного простору і забезпечення національної системи інформаційної безпеки України: по-перше, удосконалити нормативно-правову базу у сфері інформаційної політики держави, яка б визначала взаємодію силових структур України з органами місцевого самоврядування, державними органами та громадськими інституціями; по-друге, створити єдиний міжвідомчий координаційний орган, який би здійсню-

вав керівництво, координацію та контроль заходів інформаційної безпеки, (його, наприклад, можна створити у вигляді міжвідомчої комісії при РНБО); по-третє, створити систему комплексного моніторингу популярних аудіовізуальних та друкованих ЗМІ, а також популярних Інтернет-ресурсів; по-четверте, заохочувати подальші комплексні наукові дослідження у сфері інформаційної безпеки.

Необхідно зауважити, що система інформаційної безпеки держави є складовою частиною загальної системи національної безпеки країни, представляє собою сукупність органів державної влади, недержавні структури і громадяни, які повинні узгоджено здійснювати діяльність по забезпеченню інформаційної безпеки на основі єдиних правових норм, ефективно протистояти інформаційним загрозам у сучасних умовах.

Список використаної літератури

1. Гуржій Т. Інформаційне право: виклики гібридної війни. *Зовнішня торгівля: економіка, фінанси, право*. 2018. №4. С. 16–26.
2. Дмитренко М. А. Проблемні питання інформаційної безпеки України. *Міжнародні відносини. Серія Політичні науки*. 2017. № 17. С. 236–243.
3. Косогов О. М., Сірик А. О. Завдання захисту національного інформаційного простору за досвідом ведення гібридної війни РФ на Сході України. *Системи озброєння і військова техніка*. 2017. С. 38–41.
4. Доктрина інформаційної безпеки України: затверджено Указом Президента України від 25.02.2017 № 47/2017. URL: <http://zakon.rada.gov.ua/laws/show/47/2017>.
5. Белай С. В., Корнієнко Д. М. Інформаційна безпека сьогодення – невід’ємна складова воєнної безпеки. Актуальні проблеми управління інформаційною безпекою держави. Київ: Національна академія Служби безпеки України, 2018. 408 с.
6. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. *Вісник НАДУ*. 2013. №3. С. 40–45.

Косогов О.М.

кандидат військових наук
старший науковий співробітник,
провідний науковий співробітник

СТРАТЕГІЇ ТА СПОСОБИ НЕГАТИВНИХ ІНФОРМАЦІЙНИХ ВПЛИВІВ ЯК СКЛАДОВИХ НЕПРЯМИХ ДІЙ В УМОВАХ МІЖДЕРЖАВНИХ КОНФЛІКТІВ

В умовах формування нового світового порядку, коли центри ваги боротьби на міжнародній арені переносяться в інформаційно-комунікаційний простір, від українських державних інститутів потрібне вміння вчасно виявляти негативні тенденції в розвитку міжнародної і внутрішньої обстановки з метою їх ефективної нейтралізації. Відсутність в державній системі відповідних організаційних структур і розроблених концепцій забезпечення національної безпеки, адекватних реаліям геополітичного протистояння, прирікає країну на втрату свого суверенітету і її руйнування як самостійного державного утворення.

Мета негативного інформаційного впливу полягає в змушенні державою-об'єктом впливу прийняти правильне з точки зору держави-комунікатора бажане для неї рішення. На практиці це полягає у застосуванні системи організаційних, пропагандистських, психологічних, інформаційних впливів на державу-об'єкт впливу, які змушують його рухатися в необхідному для протилежної сторони напрямку. Такі впливи належать до категорії "непрямих дій", термін якої було введено англійським військовим теоретиком Безіл Генрі Ліддел Гартом [1] та американським політологом Джозефом Найєм, який розширив сферу стратегії непрямих дій за рахунок залучення арсеналу політичних, дипломатичних, економічних, психологічних та інформаційних методів [2]. У результаті скоординованих дій в державі-об'єкті непрямих дій має виникнути віртуальний продукт, наратив, спрямований на стимулювання конкретних дій щодо створення ситуації внутрішньополітичного, економічного і психологічного хаосу.

Український дослідник Г. Почепцов називає такий тип наративу мобілізуючим, здатним об'єднати суспільство для рішучих змін існуючого порядку [3].

Володимир Путін ще восени 2014 року заявив: “Росія буде втручатися в українські справи на тій підставі, що український народ є частиною “великого російського світу”, українська держава - помилка історії, штучно створене “складносурядне державне утворення”, а оскільки в Україні кровопролиття, громадянська війна, катастрофа, обов’язок Росії цю ситуацію виправити” [4].

На рівні офіційних документів Росія постійно декларує принципи використання “м’якої сили” в зовнішній політиці [5–7].

У зв’язку з цим набуває особливої актуальності проблема виявлення технологій негативного інформаційного впливу як складової непрямих дестабілізуючих впливів.

Функціонування держави як соціально-економічної системи (СЕС) можна описати через динаміку її основних характеристик [8]:

$$\frac{dx}{dt} = f\{t, X(t), F(X(t - \tau)), u(t, W, Z, E)\} = f\{X, a\} \quad (1)$$

де X – вектор змінних, що характеризують стан держави;

$F(X(t - \tau))$ – функціонал, що враховує вплив на поточний стан системи її попередніх станів (пам’ять, традиції, інерційність реакції системи на дії тощо);

$u(t, W, Z, E)$ – керуючі впливи на систему органів управління держави;

W – вектор основних напрямків функціонування держави;

Z – цільова функція органів управління державою, що характеризує бажаний стан держави;

E – ефективність реалізації органами управління державою поставленої мети;

a – сукупність параметрів моделі.

Нехай в фазовому просторі системи (1) є два стійких її стану (аттрактора), з яких кращим у системі прийнятих критеріїв (політичних, економічних, соціальних) є аттрактор A_2 (рис.1). Якщо стан СЕС в момент часу t_0 відповідає точці 1 в фазовому просторі, то орган управління прагне направити еволюцію системи в напрямку

аттрактора A_2 . За допомогою дестабілізуючих впливів різного виду можна перешкодити такому розвитку подій і домогтися ослаблення СЕС (у математичній постановці це означає переміщення фазового стану системи в область тяжіння аттрактора A_1).

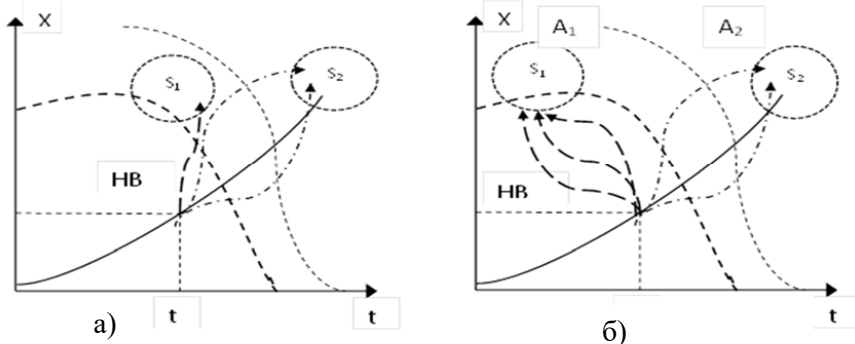


Рисунок 1 – Зміна структури фазового простору систем: а) – стан фазового простору до і після дестабілізуючих впливів за першим способом; б) – стан фазового простору до і після дестабілізуючих впливів у інший спосіб.

Основними видами дестабілізуючих впливів є:

а) силовий вплив (застосування військової сили або загроза її застосування);

б) економічний вплив (ембарго, торгові війни, нерівноправні економічні договори, перешкоджання розвитку національної економіки тощо);

в) організаційний – вплив на органи державного і військового управління інформаційний простір, усі сфери суспільного життя).

Дестабілізуючі впливи можуть бути реалізовані трьома основними типами трансформації СЕС (1), що призводять до її ослаблення і дестабілізації:

- 1) навмисна зміна вигляду системи (1);
- 2) зміна будь-яких параметрів а системи (1);
- 3) змішання фазової траєкторії СЕС шляхом зовнішнього дестабілізуючого впливу.

Розглянемо послідовно стратегії ослаблення і дестабілізації держави.

Стратегія 1. Навмисна зміна вигляду системи $f \rightarrow f'$

Ця стратегія полягає в трансформації системи (1) таким чином, щоб в її фазовому просторі зник аттрактор A_2 (рис.1). Цього можна досягти двома основними способами.

Перший полягає в заміні системи (1) на іншу, у якій аттрактор A_2 відсутній. Реально це виражається в зміні форми правління, способів організації суспільства і держави.

Другий спосіб передбачає зміні структуру системи (1) (тобто явної ланки сформованих соціально-економічних і політичних структур не відбувається), однак до СЕС підключається підсистема $Y(t)$, яка реалізує свою траєкторію розвитку ($dY/dt = h\{t, Y, \mu\}$) і нав'язує її основній системі:

$$\frac{dX}{dt} = f\{t, X(t), F(X(t - \tau)), u(t, W, Z, E)\} + \varepsilon\{y - x\} \quad (2)$$

$$\frac{dY}{dt} = h\{t, Y, \mu\} + \delta\{x - y\} \quad (3)$$

де ε і δ – матриці зв'язку підсистеми $Y(t)$ із системою (1).

Реально це виражається у впровадженні активних елементів в структуру, що впливають на прийняття стратегічних рішень (уряд, політична і економічна еліта, керівництво ЗМІ тощо).

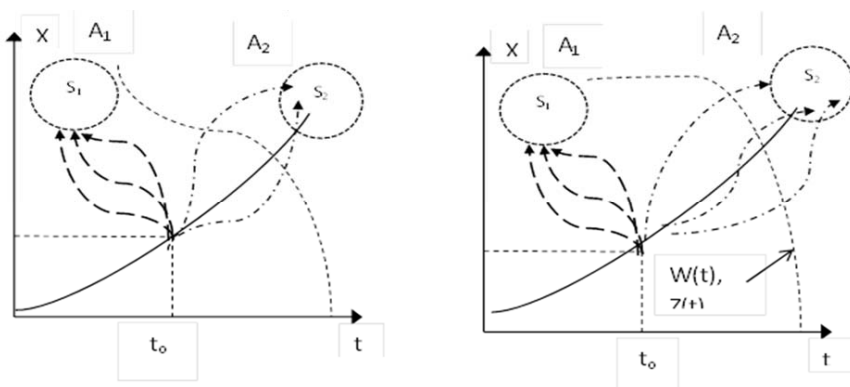


Рисунок 2 – Зміна структури фазового простору СЕС згідно із стратегією 2.

Стратегія 2. Зміна параметрів системи (1): $a \rightarrow a'$. Ця стратегія полягає в зміні параметрів системи (1), що впливають на стан сепаратріси, яка розділяє області притягання G^1 і G_2 (рис.2). Метою впливу є зміщення сепаратріси таким чином, щоб система виявилася в області тяжіння менш сприятливого аттрактора A_1 (рис. 2(б)).

Іншими словами, метою впливу є така зміна параметрів системи (наявної ресурсної бази W , характеру взаємодії підсистем, цільової функції Z центральних і місцевих органів управління тощо), щоб система сама, без видимого зовнішнього примусу стала еволюціонувати до аттрактору A_1 . Цього можна домогтися такими способами.

Спосіб 2.1. полягає в зміні значення будь-якого параметра (або групи параметрів) з одного рівня на інший, що супроводжується довготривалим зміщенням сепаратріси. Цього можна досягти за допомогою:

зменшення ресурсної бази W військовим або невійськовим (наприклад, економічним) шляхом;

зміни довгострокових цілей уряду (тобто його цільової функції Z) у результаті військового, або невійськового (економічного, організаційного інформаційно-психологічного та іншого) тиску;

зміни соціально-психологічної ситуації в суспільстві (цільових установок населення) в результаті його інформаційно-психологічної обробки через засоби масової інформації.

Спосіб 2.2. полягає в імпульсному зміні значення будь-якого параметра (або групи параметрів), що супроводжується часовим зсувом сепаратріси.

Цього можна досягти, наприклад, організовуючи періодичні фінансові кризи (економічний вплив) або викликаючи соціально-політичну нестабільність в суспільстві шляхом вкидання в ЗМІ різного роду дестабілізуючої дезінформації (організаційний вплив).

Спосіб 2.3. полягає в вибірковій дестабілізації зв'язків (економічних і організаційних) між окремими підсистемами і регіонами призводить до дестабілізації управління і провокування внутрішніх конфліктів (організаційний вплив).

Спосіб 2.4. Збільшення часу запізнювання реакції системи (і в першу чергу, органів управління) на дестабілізуючі дії. Збільшення часу запізнювання знижує ефективність управління і може пере-

вести систему в хаотичний режим. Такий спосіб дестабілізації реалізується в результаті організаційного впливу на систему.

Спосіб 2.5. має на увазі адаптивне зовнішнє управління параметрами системи:

$$\frac{dX}{dt} = f\{X, a(t)\}, \quad (4)$$

$$\frac{da}{dt} = -\gamma(X - X_s) \quad (5)$$

де – стан системи (1), реалізації якого хоче добитися протидіюча сторона.

Стратегія 3. Примусова зміна траєкторії системи.

Ця стратегія полягає в примусовому зміні траєкторії системи (1) в напрямку аттрактора A_1 (рис 3). При цьому цільова функція Z органу управління системи (1) залишається незмінною (прагнення до аттрактору A_1), проте реалізувати своє прагнення орган управління не в змозі.

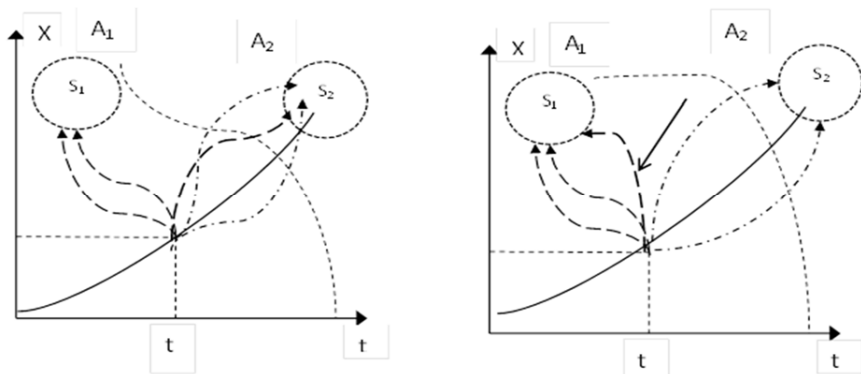


Рисунок 3 – Зміна структури фазового простору СЕС– стан фазового простору до (а) і після (б) дестабілізуючих впливів третього типу

Спосіб 3.1. полягає в прямому (силовому) зміщенні траєкторії $X(t)$ в результаті надання ворожих військових або невоєнних (економічних, організаційних) впливів.

Спосіб 3.2. полягає у використанні керуючих впливів спеціального виду зі зворотним зв'язком для впливу на траєкторію $X(t)$. Управління здійснюється за допомогою економічного, політичного примусу за допомогою нав'язування нерівноправних угод і договорів (економічного та організаційного впливів).

Спосіб 3.3. полягає в непрямому впливі на траєкторію $X(t)$ шляхом створення перешкод ефективному функціонуванню системи (1) та її органів управління. Такий спосіб дестабілізації реалізується в основному в результаті організаційного впливу на систему і створення військових загроз.

Таким чином, мета НД максимально підпорядкувати противника інтересам суб'єктів негативного впливу.

Список літератури

1. Б. Г. Лиддел Гарт, Энциклопедия военного искусства. Стратегия не прямых действий, Москва, Санкт-Петербург: АСТ, Терра Фантастика 2003, с. 656.

2. J. S. Nye, Bound to Lead: the Changing Nature of American Power, New York: Basic Books 1990, 336 p.

3. Г. Почепцов, Від facebooku і гламуру до WikiLeaks, Київ 2012, с. 333.

4. В. Путин, Мировой порядок: новые правила или игра без правил? Заседание Международного дискуссионного клуба «Валдай», 24 октября 2014 года, <http://kremlin.ru/news/46860> Концепция внешней политики Российской Федерации. Утверждена Президентом Российской Федерации В. В. Путиным 12 февраля 2013 г., http://www.mid.ru/brp_4.nsf/0/6D84DDEDED7DA644257B160051BF7F12.10.2014.

5. Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации от 12 мая 2009 г., <http://www.scrf.gov.ru/documents/99.html>, 10.10.2014.

6. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации В. Путиным 9 сентября 2000 г., http://www.rg.ru/oical/doc/min_and_vedom/mim_bezop/doctr.shtm,

7. Ивлев А.А. Основы теории Бойда. Направления развития, применение и реализация. М.: 2008.

Ковалів М.В.

кандидат юридичних наук, професор
завідувач кафедри адміністративно-правових дисциплін юридичного факультету Львівського державного університету внутрішніх справ

РОЛЬ ТЕХНІЧНИХ ГАРАНТІЙ ПРАВ ЛЮДИНИ ПРИ ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

З розвитком інформаційних і комунікаційних технологій загострюються проблеми забезпечення інформаційної безпеки. Йдеться про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електронного зв'язку, пропаганда сепаратизму та екстремізму тощо.

При забезпеченні інформаційної безпеки в цифровому середовищі зростає роль техніко-юридичних гарантій прав людини, за рахунок технічних засобів захисту. Покладання на розробників технічних засобів обов'язків визначає відмінність вищевказаних концепцій від традиційного підходу до забезпечення захисту прав людини, при якому обов'язки покладаються на інформаційних посередників, власників конфіденційної інформації [1, с. 1008].

Технічні гарантії прав людини стають необхідною складовою забезпечення інформаційної безпеки, але ефективність застосування забезпечується у поєднанні з правовими гарантіями прав людини, на що вказує тенденція визнання принципів недоторканності приватного життя на основі проектних рішень у праві Європейського Союзу в якості правових.

Забезпечення інформаційної безпеки виступає легітимною метою встановлення обмежень прав людини, оскільки це може бути співвіднесено з нормами міжнародного права. Встановлення обмежень прав людини допускається для досягнення інших цілей – забезпечення державної безпеки, публічного порядку, здоров'я, прав і свобод особи в інформаційній сфері. Легітимність цієї мети визначається її відповідністю цілям, передбачених міжнародними договорами, ратифікованими у встановленому порядку.

У зв'язку з активним використанням інформаційно-телекомунікаційних систем та технологій, зокрема, Інтернет, зросла кількість загроз мережових атак з метою несанкціонованого доступу в автоматизовані інформаційні системи державних і комерційних організацій для отримання конфіденційної інформації, забезпечення збоїв в роботі систем, перехоплювання управління критично важливими об'єктами.

Доктрина інформаційної безпеки України розглядає забезпечення інформаційної безпеки як один з видів діяльності і як засіб діяльності, спрямованої на безпечне функціонування та розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір. Таку діяльність здійснюють громадяни, інститути громадянського суспільства та державні органи, забезпечуючи життєво важливі інтереси особи, суспільства та держави в інформаційній сфері.

У країнах ЄС інформаційна безпека спрямована на створення умов, при яких забезпечується стан захищеності прав людини в інформаційній сфері, як основна мета і цінність інформаційної безпеки. В результаті інформаційна безпека стає однією з гарантій прав людини та громадянина в інформаційній сфері.

Під гарантіями прав людини та громадянина розуміють систему умов, засобів і способів, за допомогою яких забезпечуються рівні можливості для здійснення, забезпечення охорони та захисту прав людини та громадянина. Забезпечення інформаційної безпеки як гарантія прав людини нерозривно пов'язана з іншими видами гарантій і в них знаходить своє вираження. Комітет Міністрів Ради Європи в Рекомендації CM/Rec(2014) («Посібник з прав людини для Інтернет-користувачів») зазначає, що існуючі права людини та основні свободи в рівній мірі відносяться як до оффлайн, так і до он-лайн простору. Ніхто не повинен бути об'єктом незаконного втручання в здійснення прав людини і основних свобод під час перебування в Інтернеті [2]. Комплекс гарантій, якими забезпечується здійснення і захист прав людини в оффлайн середовищі, поширюється на права людини в кіберпросторі і цифровому середовищі.

Л. Тарасенко зазначає, що цифрове середовище – це ширше поняття, ніж мережа Інтернет. Цифрове середовище включає у себе

не лише веб-сайти (і веб-сторінки як складові веб-сайтів), а й електронні документи, файли, в тому числі оцифровані об'єкти інтелектуальної власності [3].

Умови захисту прав людини в цифровому і оффлайн середовищах розрізняються. З погляду на Стратегію кібербезпеки України, для цифрового середовища характерні технічні гарантії прав людини, які представлені у формі технічних і програмних засобів і технічних норм. Технічні та програмні засоби (далі – технічні засоби) охоплюють обчислювальні машини та спеціалізовані пристрої на їх основі, операційні системи, системи програмування, загальносистемне та прикладне програмне забезпечення [4, с. 121]. Техніко-юридичні норми визначають умови проектування, виготовлення та використання технічних засобів. При забезпеченні інформаційної безпеки в цифровому середовищі зростає роль техніко-юридичних (далі технічних) гарантій прав людини, за рахунок технічних засобів захисту. У зазначеному аспекті, доцільно погодитися з думкою О. Харитонової та інших вчених, що Інтернет-відносини це новий тип суспільних відносин, які виникають, змінюються та припиняються в кіберпросторі [5, с. 160].

Технічні гарантії прав людини стають необхідною складовою забезпечення інформаційної безпеки, але ефективність застосування забезпечується у поєднанні з правовими гарантіями прав людини.

П. Сухорольський зазначає, що за останні роки звичним для багатьох став факт, що оператори пошукових систем чи соціальних мереж мають власну політику щодо свободи і обмежень в Інтернеті та накладають обмежувальні заходи на основі самостійно розроблених критеріїв і способів бачення міжнародних проблем. Це свідчить про поступове набуття ними функцій із регулювання суспільних відносин [6, с. 346].

Технічні засоби можуть виступати гарантією прав людини тільки при наявності правових гарантій, які надають механізми правового захисту від їх довільного використання. Такі правові гарантії забезпечуються державою у межах здійснення функції забезпечення безпеки суспільства в цілому та реалізуються на підстав Законів України від 15.01.2015 № 124-VIII «Про технічні регламенти та оцінку відповідності», від 05.06.2014 № 1314-VII «Про метрологію та метрологічну діяльність», інших нормативно-правових актів.

Література

1. Ковалів М.В., Єсімов С.С., Сопільник Р.Л., Скриньковський Р.М. Гарантії прав людини та громадянина при забезпеченні інформаційної безпеки. *Traektoriâ Nauki Path of Science*. 2018. Vol. 4. № 5. S. 1008-1016.
2. Права людини в Інтернеті // Науково-методичний центр інклюзивної освіти. 07.12.2016. [Електронний ресурс]. – Режим доступу: <http://nmcio.ipro.kubg.edu.ua/?p=2213>
3. Тарасенко Л. Цифрове середовище як місце здійснення прав інтелектуальної власності / Л. Тарасенко // Центр дослідження інтелектуального права. 05.12.2017. [Електронний ресурс]. – Режим доступу: <http://ipcenter.lviv.ua/%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%>
4. Павлиш В. А. Основи інформаційних технологій і систем: навч. посіб. Львів, Вид-во Львівської політехніки, 2013. 500 с.
5. Харитонova О.І. Проблемні питання визначення правової природи і структури правовідносин інтелектуальної власності, що виникають у мережі Інтернет. *Наукові праці НУ ОЮА*. 2015. С. 159-200.
6. Сучасні проблеми міжнародного права. *Liber Amicorum* до 60-річчя проф. М.В. Буроменського / Авт. кол.; за ред. В.М. Репецького та В.В. Гутника. Львів; Одеса: Фенікс, 2017. 564 с.

Лепіш Н.Я.

кандидат юридичних наук,
доцент кафедри адміністративно-
правових дисциплін юридичного
факультету ЛьвДУВС

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНЕ ПРОТИБОРСТВО ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Інформаційно-психологічне протиборство як певна методологія зміни картини світу в заданому напрямі стало нині однією з форм боротьби передових держав, що демонструє стрімкий розвиток. Об'єктом впливу можуть бути як окремі особи або групи осіб, котрі приймають рішення на різних рівнях (кожен на своєму), так і масова свідомість нації в цілому. У політичній сфері в інформаційно-психологічному протиборстві для впливу на думки, настрої і зрештою на поведінку протилежної сторони використовують інформаційні, дипломатичні, військово-демонстраційні, економічні та інші важелі.

З-поміж особливостей інформаційно-психологічного впливу принциповими вбачаються такі: – відсутність територіальних обмежень, що дозволяє долати кордони між державами, уражаючи свідомість противника; – здійснення без видимих слідів: об'єкт впливу вважає, що він самостійно ухвалює те чи інше рішення, насправді ж його скеровують до прийняття саме цього рішення; – відносна економічність для ініціаторів, оскільки невелика за обсягом вхідна інформація може забезпечити максимально значущий результат, наприклад, формування потрібної громадської думки; – можливість різних (аж до діаметрально протилежних) інтерпретацій одного й того ж факту; – неможливість блокування дій противника в інформаційній боротьбі, навіть за умов наявності найсучасніших ІКТ (на відміну від симетричної відповіді в разі використання традиційних видів зброї) [2, с. 178].

Інформаційно-психологічна війна є найгострішою формою протиборства в інформаційно-психологічній сфері, здійснюваного шляхом впливу на цю сферу противника з метою вирішення

стратегічних завдань. Серед іншого це передбачає цілеспрямоване і планомірне використання інформаційно-психологічних інструментів та інших засобів (дипломатичних, військових, економічних та ін.) для впливу на думки, настрої і в кінцевому підсумку на поведінку противника з метою змусити його діяти в бажаному напрямі. Таким чином, інформаційно-психологічний вплив (ІПВ) – це застосування інформаційно-психологічних засобів для впливу на психіку людини з метою коригування в потрібному для суб'єкта впливу напрямі і внесення змін до поведінки та/або світогляду. Головним критерієм успішності ІПВ виступає результат цього процесу, що може виражатися у вигляді зміни настанов, поведінки, намірів та оцінок конкретного індивіда або групи осіб.

Основною формою ведення і головним елементом змісту інформаційно-психологічної війни є інформаційно-психологічна операція – сукупність видів, форм і способів інформаційного впливу, узгоджених, скоординованих і взаємопов'язаних за цілями, завданнями, місцем, часом, об'єктами і процедурами. Інформаційно-психологічні операції розрізняються за масштабами, цілями й завданнями, об'єктами впливу, використовуваними технологіями та умовами проведення. За термінами здійснення інформаційно-психологічні операції поділяють на: стратегічні (довгострокові); оперативні (середньострокові); тактичні (короткострокові).

За часом здійснення: на операції, що проводяться до переходу конфлікту в силову фазу; такі, що реалізуються в умовах активного зіткнення.

За спрямованістю виокремлюють операції: спрямовані безпосередньо проти реципієнта; такі, що проводяться в інтересах комунікатора, або операції проти третіх осіб з метою схилити їх на свій бік.

Своєю чергою, інформаційно-психологічні методи й засоби психотехнологій класифікують на відкриті й приховані (таємні), позитивні й негативні, такі, що переслідують явні та приховані цілі.

Таємні інформаційно-психологічні операції однієї держави або ж групи держав проти іншої (інших) реалізуються через здійснення спрямованого інформаційного впливу на індивідуальну, групову, масову свідомість, почуття, волю громадян, а також шляхом

дезінформування суб'єктів прийняття політичних, економічних та іншого роду рішень і підризу інформаційної інфраструктури су-противної сторони.

Мета подібних операцій – створити умови, за яких у військовій, політичній, економічній та інших сферах країн – об'єктів інформаційно-психологічного впливу ухвалюватимуться управлінські рішення, вигідні для держав – організаторів цього впливу. Щоби сформувати такі умови, спеціально підготовлена інформація доводиться до об'єктів впливу за допомогою електронних, друкованих та інших засобів масових комунікацій, електронного й поштового зв'язку, аудіо-, відео- та кінопродукції, відкритих телекомунікаційних мереж, наочно-демонстраційних засобів і т. ін. [3, с. 39].

На сучасному етапі боротьби держав за сфери впливу акцент із явного застосування сили усе помітніше зміщується на використання більш гнучких засобів, основним із яких є контроль і керування інформаційними ресурсами. Для досягнення цих цілей в умовах зростаючої насиченості інформаційними й керуючими засобами, у тому числі й іноземного виробництва, може бути використане високоефективне таємне проникнення у програмне забезпечення державних інформаційних ресурсів. Українські правоохоронці постійно нагадують, що злочинці намагаються зламати інформаційні мережі й поштові сервери державних установ. Під виглядом офіційних листів надсилаються електронні повідомлення із вкладеним шкідливим програмним забезпеченням, яке рекомендується встановити. Зокрема, СБ України неодноразово звертала увагу керівників державних органів влади та установ, а також співробітників ІТ-департаментів на необхідність посилення заходів з недопущення несанкціонованого встановлення програмного забезпечення чи його оновлення, аби не допустити хакерського проникнення на державні інформаційні ресурси.

Крім того, висока результативність використання інформаційно-телекомунікаційних систем і технологій, широкий спектр їх застосування і прихований характер дії зумовили те, що багато країн ведуть розробки в галузі теорії та практики їх застосування як інформаційної зброї і, як наслідок, теорії ведення інформаційних війн [4, с. 45].

Стрімкий розвиток технологій роботи з інформацією в розвинених країнах зумовлює формування стратегій «інформаційної війни», головною метою якої є інформація, оволодіння нею чи трансформація у своїх інтересах.

Очевидним стає той факт, що в сучасних умовах інформаційні технології відіграють надзвичайно важливу роль не тільки в забезпеченні національної безпеки, а й у розвитку особистості, суспільства й держави [1].

Підсумовуючи аналіз теорій правового забезпечення інформаційної безпеки держави, зазначимо, що перші спроби людини зберегти таємність будь-якої інформації поклали початок формуванню теоретичних основ інформаційної безпеки. З розвитком технологій і обсягів передачі даних змінювалися методи захисту інформації. Як бачимо, на сучасному етапі розвитку суспільства ефективне забезпечення інформаційної безпеки дозволяє вирішувати ключові питання практично всіх видів національної безпеки. Інформаційна безпека є важливою складовою системи національної безпеки, і від успішного вирішення питань даної сфери залежить забезпечення глобальної загальносвітової безпеки.

Список використаної літератури

1. Доктрина інформаційної безпеки. URL: <http://hromadske.ua/posts/doktrina-informaciinoi-bezpeki>
2. Лісовська Ю.П. Державна політика забезпечення інформаційної безпеки України: адміністративно-правовий аспект. Молодий вчений. 2015, № 2 (17). С.177-179
3. Ткачук Т. Ю. Державна політика у сфері забезпечення інформаційної безпеки на сучасному етапі. Наук. вісник УжНУ. Серія «Право». 2017. № 46. Т. 2. С. 39–43.
4. Ткачук Т. Ю. Інформаційна безпека: сучасні підходи до визначення категорії. Актуальні питання публічного та приватного права. 2017. № 2 (16). С. 45–54.

Кронівець Т.М.

кандидат юридичних наук, ст. викладач кафедри правових наук та філософії Вінницького державного педагогічного університету імені Михайла Коцюбинського

ЗАХИСТ ПРИВАТНОСТІ ЖИТТЯ ЛЮДИНИ В ІНФОРМАЦІЙНОМУ СУСПІЛЬСТВІ: ОСОБЛИВОСТІ ПОНЯТІЙНОГО АПАРАТУ

В статті розглядається питання правового захисту приватності життя людини в інформаційній сфері. На підставі аналізу норм законодавства, наукових розвідок провідних правників проведено дослідження понятійного апарату, окреслено межі дефініцій, визначено їх зміст. Наголошено на необхідності комплексного вивчення питання приватності життя людини з метою вироблення єдиної концепції захисту. Вказано на важливість даного питання для захисту особистих та національних інтересів.

Ключові слова: приватність життя людини, захист прав, буття людини, персональні дані, інформаційне суспільство.

Питання приватності життя людини було предметом наукових розвідок соціологів, філософів, економістів тощо. Із розвитком інформаційного суспільства в світі загалом, та в Україні зокрема, питання приватності життя людини стало предметом дискусій правників.

Відсутність дієвих механізмів захисту приватності людини, в тому числі персональних даних в інформаційній сфері призводить до загроз не тільки особистим правам, але й національній безпеці держав. Питання захисту приватності кожної людини акумулює в собі правові, філософські, економічні та моральні проблеми, що потребують ефективного вирішення. Зацікавленість вітчизняних науковців проблемами інформаційного права втілилась у фундаментальних дослідженнях, зокрема щодо захисту персональних даних, однак межі приватності людини набагато ширші, якщо взагалі можуть бути охоплені. Таким чином, актуальність питання захисту

приватності життя людини в інформаційній сфері та відсутність комплексних досліджень за обраною тематикою зумовлює потребу дослідити це питання з правової точки зору.

Приватність життя людини це та правова та філософська категорія, що аж ніяк не обмежується життям сімейним чи особистим. Віднесемо до даного поняття персональні дані, право ними володіти, користуватися, розпоряджатися, визначати їх зміст. Честь, гідність, недоторканість і безпека людини також складають невідзначене коло понять, що варто долучити до питання приватності. Взаємодія в соціальному та віртуальному просторі, право на вибір, на самовизначеність, ідентичність, моральність, гендер – на нашу думку, також складає приватність життя людини.

Поняття «приватності» не знайшло свого відображення у вітчизняному законодавстві. Однак, основний закон держави визначає, що «людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю» [1, ст.3]. Далі вказано, що «кожна людина має право на вільний розвиток своєї особистості, якщо при цьому не порушуються права і свободи інших людей, та має обов'язки перед суспільством, в якому забезпечується вільний і всебічний розвиток її особистості» [1, ст.23]. На нашу думку, це твердження найповніше в законодавстві може визначати межі «приватності». Тут чітко окреслена межа між правом людини і обов'язком перед суспільством. Приватність – це гарантоване державою право людини вільно і всебічно реалізовуватись, в межах допустимих власною моральністю та законом.

Поступово зароджуючись у 1890 році із права особи «на саму себе», «права на самотність» [2, с.15] приватність у ХХІ ст. стає визначальною правовою категорією, способом вираження людської особистості і мірою відповідальності держави.

Приватність особи це внутрішня сторона її буття, право людини бути унікальною особистістю, що виражає себе у просторі. Вчені констатують появу нової форми буття – «віртуальної реальності». Це призводить до вивчення в онтології нового явища – «ірреальності буття» [3, с.11].

В правовому просторі приватність виражається через вільне створення людиною власної індивідуальності, поширення інфор-

мації про власну персону, обмеження чи заборону поширення відомостей, можливість контролю над якістю, наповненням контенту, в якому згадується людина, можливість притягнення до відповідальності осіб, винних у порушенні приватності людини тощо. Вторгнення до житла з метою крадіжки речі чи з метою крадіжки інформації про спосіб життя, звички людини – однаково порушують приватний простір людини, шкода завдана від оприлюднення фото житла людини набагато перевищує шкоду від викрадення телевізора.

Визначення обсягу інформації, що потребує захисту відбувається через призму усвідомлення людиною цінності інформації і можливостей неправомірного її поширення. Обмеження людиною права вільно збирати відомості про себе (шляхом визначення правил конфіденційності в соціальних мережах, наприклад), зберігає приватність не лише їй, але й її близькому оточенню.

Таким чином, можна констатувати, що межі захисту приватності людини містяться в кількох площинах: приватні чи особисті (самозахист), інституційні (захист в спільності, корпорації), державні (гарантований нормативний мінімум).

Прерогатива початкового визначення меж приватності належить державі, в правовому полі якої здійснюється взаємодія людини з соціумом, а остаточного –самій людині, що має відповідну дієздатність приймати рішення в кожному конкретному правовідношенні.

Вважаємо, що приватність це частина правосуб'єктності особи, невід'ємна від її буття. При цьому варто зауважити, що межі приватності можуть виходити за межі фізичного життя людини, оскільки в окремих випадках захищається приватність ненародженої дитини (дискусії щодо правового статусу ембріона тривають), і приватність людини після її смерті.

Структуруючи поняття приватності можемо зауважити, що обов'язковою ознакою єї невіддільність від суб'єкта – фізичної особи. До змінних ознак належать етнічні, релігійні аспекти, ментальність, моральна ідентифікація особи, площина вираження (реальна, віртуальна), сфера захисту тощо.

Погоджуючись, що «інформаційне суспільство є необмеженим простором для самоконструювання особистості» [4, с.12], вважа-

ємо, що взаємодія людей в інформаційному просторі, в його фундаментальному значенні, створює площину, що потребує нових правових механізмів захисту. Захист права на приватність людини відбувається виключно в інформаційній площині. Людина, що перебуває поза межами соціуму чи/ та в інформаційному вакуумі також потребує захисту права на приватність, зокрема, шляхом надання їй вибору –взаємодіяти чи ні.

Захист права на приватність в інформаційній сфері включає в себе можливість реалізації права, визначення меж приватності, зокрема право бути забутим, створення механізму припинення порушення приватності особи, чітке визначення складів правопорушень та дієву процедуру притягнення до відповідальності осіб, винних у порушенні приватності людини, та розробку превентивних заходів, зокрема систему правового виховання людини в дусі поваги до приватності.

Список використаних джерел

1. Конституція України від 28 червня 1996р. (із змінами) [Електронний ресурс] // Режим доступу: <https://zakon.rada.gov.ua/laws/show/254к/96-вр>.
2. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / [В.Г. Пилипчук, В.М. Брижка, О.А. Баранов, К.С. Мельник] ; за ред. В.М. Брижка, В.Г. Пилипчука. – К. : ТОВ «Видавничий дім «АртЕк», 2017. – 226 с.
3. Брижка В.М., Фурашев В.М. Інформаційне право та інформаційне законодавство: наукове видання. – (НДПП НАПрН України). – Київ: Видавничий дім “АртЕк”, 2020. – 288 с.;
4. Дзьобань О. П. Людина в інформаційному суспільстві: проблема моральної ідентифікації. // Вісник національного юридичного університету імені Ярослава Мудрого – №1 (40).– 2019 . – С.9-20.

Яременко О.І.

кандидат наук з державного управління,
доцент,
завідувач кафедри правових наук та
філософії Вінницького державного
педагогічного університету імені
Михайла Коцюбинського,

ПРАВОВІ ЗАСАДИ ІДЕНТИФІКАЦІЇ ТА АУТЕНТИФІКАЦІЇ ФІЗИЧНИХ ОСІБ ЯК СУБ'ЄКТІВ ВІРТУАЛЬНИХ ІНФОРМАЦІЙНИХ ВІДНОСИН

Високі темпи розвитку технологій в інформаційно – комунікаційній сфері призвели до появи нових типів соціальної взаємодії та трансформації переважної більшості видів діяльності людини. Впровадження інформаційно – комп'ютерних технологій змінює традиційні уявлення про матерію, простір та час, створює нові форми та виміри соціального буття і світосприйняття. Як наслідок, паралельно з об'єктивним фізичним світом та суб'єктивними уявленнями про нього, виникає нова реальність, яка отримала назву «віртуальної», а паралельно з традиційним матеріальним простором інституалізується простір віртуальний.

В сучасних умовах відбувається активна міграція багатьох суспільних відносин у віртуальний (кібернетичний) простір, в якому відбувається як особисте спілкування, так і управлінська, інформаційна, освітня, наукова, юридична та інші види діяльності. При цьому, просторова віддаленість і відсутність безпосереднього контакту між учасниками віртуальних відносин, породжує проблему їх ідентифікації, що актуалізує наукові дослідження в цій сфері.

Метою даної статті є аналіз правових проблеми ідентифікації та аутентифікації фізичних осіб як суб'єктів віртуальних інформаційних відносин.

На сьогодні, феномен віртуальності є надскладним технологічно – соціальним явищем, яке містить в собі різноманітні аспекти і характеризується поліваріативністю об'єктивних форм та зовнішніх проявів. Як слушно зазначає Дзьобань О.П., категорія “віртуаль-

ний світ” втілює у собі подвійний сенс – уявність (вигаданість) та справжність (істинність) одночасно. Віртуальна реальність – це мережевий феномен, що свідчить про новий тип просторово-часових відносин, про уникнення ієрархічності як принципу існування систем, заміну матеріальності тілесністю, про одноплщинність мінливих змістів подій у вимірі правового дискурсу. При цьому, науковець підкреслює, що у праві, як соціальній сфері, діє логіка віртуальності. Віртуальний простір права утворюється через інформаційно-комунікативну активність суб’єктів правовідносин, кожен з яких являє свою симулятивну реальність правової ситуації. Кінцева кількість можливих світів (тобто уявних варіантів скоєння злочину, ступеня провини злочинця, фактів справи і їх доведеності, винесення справедливого вердикту) взаємодіють і систематизуються у динамічному неоднозначному синергетичному полі права [1, с.13].

Найбільш масштабним і суспільно значимим проявом віртуальної реальності є віртуальний інформаційно – комунікаційний простір, який можна кваліфікувати як транскордонне інфраструктурне електронне (цифрове) середовище, утворене надскладною динамічною системою з’єднаних стаціонарних та мобільних пристроїв, в якому, в межах технічних можливостей цих пристроїв та волевиявлення суб’єктів, здійснюються інформаційні процеси та соціальні комунікації, відбувається виконання робіт та надання послуг. Тобто у віртуальній реальності виникають, розвиваються і припиняють свою дію суспільні відносини аналогічні відносинам у фізичній реальності. Вони існують реально, породжують реальні права та обов’язки і конкретні результати і за цими параметрами мало чим відрізняються від традиційних суспільних відносин.

Фурашев В.М., розглядає кіберпростір як форму співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам’ятовування, переробку та обмін інформацією. Науковець цілком слушно підкреслює, що кіберпростір є дуже складним явищем, що об’єднує в собі реальність і віртуальність, матеріальне і нематеріальне, абстрактність і дійсність [2, с. 165].

Беляков К. І. вводить в науковий обіг поняття «віртуально – інформаційні правові відносини» і кваліфікує їх як взаємні відно-

сини двох чи більше осіб із приводу майнових благ, що породжуються обставинами виникнення та існування в інформаційно-технологічному просторі, як результат комунікації та обміну даними в електронно-цифровій формі, що визначається наднаціональними ознаками на засадах юридичної рівності та автономії волі їх суб'єктів [3, с. 22].

Еннан Р.Є. суспільні відносини, що виникають у зв'язку з використанням глобальних комп'ютерних мереж, вважає особливими інформаційними відносинами, спрямованими на організацію руху інформації у суспільстві, і підкреслює, що їх учасниками можливо бути лише за допомогою ЕОМ, підключеної до комп'ютерної мережі [4, с. 369].

Вважаємо, що феномен віртуальності створює нові прояви інформаційної поведінки людини та формати соціальних комунікацій, і, як наслідок, породжує нові типи інформаційних суспільних відносин, які мають ряд особливостей: вони здійснюються виключно через посередництво електронних пристроїв; об'єктом цих відносин є інформація, формат якої придатний для обробки програмним забезпеченням цих пристроїв; обсяги інформації, якими обмінюються учасники, фактично не обмежується; вони функціонують, в основному, в режимі реального часу (он - лайн), хоча допускається і режим оф – лайн; в них може брати одночасно невізначена кількість учасників незалежно від їх місцезнаходження; учасники можуть знаходитися під юрисдикцією різних держав і їх інформаційно – правовий статус може суттєво відрізнитися; в них допускається анонімність учасників чи участь під псевдонімом; однією із сторін може виступати носій штучного інтелекту (робот, бот, андроїд).

Технологічна природа кіберпростору дозволяє учасникам соціальної взаємодії брати в ній участь на засадах анонімності, під псевдонімом чи справжнім іменем. У будь - якому випадку, в електронному середовищі акумулюються певні ідентифікаційні дані користувачів, обсяг яких формується за волею самої особи або інших осіб на основі корпоративних чи правових норм та відповідно до умов передбачених власником (адміністратором) того чи іншого мережевого ресурсу. Під час реєстрації користувача на різноманіт-

них ресурсах формується легальний інформаційний профіль особи. Якщо ж фізична особа виступає як звичайний пасивний споживач інформації в мережі Інтернет, він залишає про себе мінімум інформації і його подальша ідентифікація можлива за спеціальними технологічними та правовими процедурами.

Система ідентифікації і аутентифікації особи є одним з ключових елементів інфраструктури захисту від несанкціонованого доступу до будь-якої інформаційної системи. Завданням систем ідентифікації і аутентифікації є визначення і верифікація набору повноважень суб'єкта при доступі до інформаційної системи. Ідентифікація дозволяє суб'єкту повідомити своє ім'я за допомогою якогось унікального, властивого тільки йому ідентифікатора (ознаки). За допомогою аутентифікації інша сторона переконується, що суб'єкт дійсно той, за кого він себе видає. Як синонім слова "аутентифікація" іноді використовують словосполучення "перевірка достовірності". Аутентифікація – це процедура, яка перевіряє, чи має користувач з пред'явленим ідентифікатором право на доступ до ресурсу [5, с. 217].

Регламент ЄС №910/2014 Європейського Парламенту та Ради від 23 липня 2014 «Про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку і скасування Директиви 1999/93/ЄС» трактує електронну ідентифікацію як процес використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну або юридичну особу або фізичну особу, що представляє юридичну особу. Під автентифікацією розуміється електронний процес, що дозволяє підтвердити електронну ідентифікацію фізичної або юридичної особи; або походження та цілісність електронних даних [6].

Особлива актуальність ідентифікації фізичних осіб обумовлюється необхідністю доступу до сучасних електронних сервісів. Надання таких послуг передбачає он-лайн взаємодію між громадянином та органом, що надає послугу через певні інтерфейси інформаційної системи з використанням механізмів електронної ідентифікації та автентифікації, які мають бути засновані на принципах безпеки та гарантій впевненості в ідентичності обох сторін такої взаємодії. Як зазначається в Європейському плані дій із електро-

ного урядування, для отримання багатьох послуг дуже важливо визначити та встановити фізичну або юридичну особу, якій надається відповідна послуга. Технології електронної ідентифікації та сервіси із встановлення особи є дуже важливими для забезпечення безпеки електронних транзакцій як у державному, так і в приватному секторі [7].

За Регламентом ЄС eIDAS електронна ідентифікація фізичних і юридичних осіб відбувається шляхом видачі їм в установленому порядку і на основі встановленої схеми спеціальних персональних засобів електронної ідентифікації (електронних карток, паспортів та інших засобів, тобто електронних ідентифікаторів, пов'язаних з конкретною особою). Головною вимогою до eID є забезпечення технологічної можливості здійснення підтвердження справжності власника електронного ідентифікатора при виконанні ним будь-яких електронних транзакцій. Ці два аспекти є обов'язковими для надання електронних послуг та здійснення електронних транзакцій. Транзакції в мережі Інтернет повинні здійснюватися за допомогою апаратного чи програмного забезпечення, оснащеного необхідним стеком технологій для генерації єдиного пан-європейського цифрового підпису.

В Україні відбувається активний розвиток адміністративних послуг в електронній формі, які надаються через Єдиний державний портал адміністративних послуг, у тому числі через інтегровані з ним інформаційні системи державних органів та органів місцевого самоврядування. Реєстрацію на цьому та інших державних електронних ресурсах можна за допомогою логіна та пароля, адреси електронної поштової скриньки, електронного підпису, системи BankID.

Серед цих варіантів ідентифікації найбільш захищеним є використання електронного цифрового підпису. Закон України «Про електронні довірчі послуги» дає визначення електронної ідентифікації як процедури використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи. Норми цього закону передбачають, що схема електронної ідентифікації повинна встановлювати три рівні довіри до засобів електронної ідентифікації, що

використовуються в них: низький (забезпечує обмежений ступінь довіри до заявлених або затверджених ідентифікаційних даних); середній (забезпечує суттєвий ступінь довіри до заявлених або затверджених ідентифікаційних даних); високий (забезпечує найвищий ступінь довіри до заявлених ідентифікаційних даних).

Подальший розвиток інститутів електронної держави та електронного врядування в Україні обумовлює необхідність вдосконалення правових норм, які регламентують питання ідентифікації та аутентифікації фізичних осіб як суб'єктів віртуальних інформаційних відносин. При цьому, важливе значення має використання досвіду Європейського Союзу щодо розбудови єдиного цифрового простору та єдиного цифрового ринку на основі системи електронних довірчих послуг. Актуальним є проблема легітимізації в Україні електронних довірчих послуг, які надаються постачальниками, які зареєстровані за законодавством іноземних держав, що може бути предметом подальших досліджень в цьому напрямку.

Література

1. Дзьобань О. П. Правовий дискурс справедливості як віртуальна реальність права / О. П. Дзьобань // Інформація і право. – 2013. – № 2. – С. 5 -16.
2. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності / В. М. Фурашев // Інформація і право. – 2012. – № 2. – С. 162 – 169.
3. Беляков К. І. Понятійні та методологічні основи регулювання нових типів інформаційних відносин: “віртуальні правовідносини” / К. І. Беляков // Lex Portus. – 2016. – № 2. – С. 47-63.
4. Еннан Р.Є. Правове регулювання відносин у мережі інтернет ІТ право: проблеми і перспективи розвитку в Україні: збірник матеріалів науково-практичної конференції. – Львів: НУ «Львівська політехніка», 2016. – 396 с.
5. Кошева Н.А., Мазниченко Н.І. Ідентифікація користувачів інформаційно-комп'ютерних систем: аналіз і прогнозування підходів / Н.А Кошева // Системи обробки інформації. – 2013. – № 6. – С. 215 – 223.

6. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC // Режим доступу: <http://data.europa.eu/eli/reg/2014/910/oj>.

7. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / Під ред. О. Потія та Ю. Козлова, 2015 // Режим доступу: <https://cdn.regulation.gov.ua/8d/f3/4c/32/regulation.gov.ua>.

Проць І.М.

кандидат юридичних наук, доцент
кафедри адміністративно-правових
дисциплін юридичного факультету
Львівського державного університе-
ту внутрішніх справ

Чабак В.Ю.

здобувач освітнього ступеня магістр
ПрАТ «ВНЗ» «Міжрегіональна ака-
демія управління персоналом»

ПРОБЛЕМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У КОНТЕКСТІ СУЧАСНОЇ КОМУНІКАЦІЇ

Україна як частина сучасного світу в даний час перебуває на етапі розвитку, що отримав наукове та нормативне визначення «інформаційне суспільство». Становлення такого суспільства обумовлено високими темпами розвитку інформаційних технологій на базі динамічних інформаційних систем, використанням глобальних телекомунікаційних мереж (Інтернет), зростанням швидкості передачі та обробки інформації, збільшенням ємності мобільних носіїв, формуванням різних електронних баз даних персональної інформації жителів України. Зазначені досягнення науково-технічного прогресу позитивно відбиваються на поліпшенні життя, оптимізації управлінських процесів, можливості реалізації конституційних прав на пошук, отримання, передачу і поширення інформації. Водночас розвиток інформаційних технологій безпосередньо впливає на стан інформаційної безпеки суспільства та окремої людини в процесі обробки персональних даних в інформаційних системах.

Захист особистих даних сьогодні – фундаментальне та досить комплексне поняття, яке, з одного боку, відображає прагнення захистити недоторканність особистого життя, з іншого – визначає його як інформацію, яка відображає участь особистості в суспільних та соціальних відносинах, що робить особисте життя доволі уразливим об'єктом щодо отримання особистих даних іншими

особами [1]. Воно відображає цілий комплекс дій з отримання та обробки інформації, яка дозволяє ідентифікувати конкретну особу. Інститут захисту персональних даних є елементом державної системи захисту інформації, що забезпечує особисту безпеку, підтримує баланс інтересів особистості, суспільства та держави у сфері обробки інформації [1].

Варто відмітити, що незважаючи на актуальність проблематики щодо захисту персональних даних, теоретична дискусія щодо змісту поняття «захист персональних даних» у науковій літературі відсутня. Дослідження вітчизняних учених зосереджені на опрацюванні та систематизації наявного нормативного поля, яке забезпечує правове врегулювання захисту персональних даних.

В нормативних джерелах по різному трактується зміст поняття «персональних даних».

Персональні дані – будь-яка інформація, яка стосується конкретно визначеної особи або особи, що може бути конкретно визначеною[2].

Інформація про фізичну особу (персональні дані) – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована[3].

Персональні дані – відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована[4].

Проаналізувавши наведені визначення свідчить про те, що в основному вони збігаються, ключовим моментом усіх визначень є можливість безпомилкової ідентифікації конкретної особи.

В основу обробки персональних даних покладено низку базових принципів (правила, що повинні дотримуватися (за незначними винятками) будь-яким володільцем у процесі здійснення будь-якої обробки), мета формулювання яких – визначення правових засад її здійснення. Вони формуються на наднаціональному та національному рівнях.

Згідно ст 32 Конституції України зазначається що: «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної

інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини» [5].

Підставою виникнення права на використання персональних даних є згода суб'єкта персональних даних на обробку його персональних даних. Відповідно до ч. 2 ст. 11 Закону України «Про інформацію» від 02.10.1992 р. [3] не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

Саме для цього і потрібні законодавчі норми щодо захисту персональних даних.

Незважаючи на гучні скандали щодо доступу та оприлюднення персональних даних та зростання критики на адресу соціальних мереж, у щоденному житті користувачі продовжують залишати чимало особистих даних (і не лише в мережі Інтернет), іноді навіть не здогадуючись про можливість використання їх третіми особами. Саме тому контроль за дотриманням правил збору, зберігання та захисту персональної інформації повинні взяти на себе державні органи. Захист персональних даних повинен враховувати усі етапи, що пов'язані з персональними даними, – від їх збирання до знищення або ж втрати ними актуальності. Базовою метою захисту персональних даних повинно бути забезпечення ключових прав та свобод громадян. Організаційно-економічною «площиною» для її реалізації повинен стати відповідний механізм, в якому основою має бути чинний Закон України «Про захист персональних даних» та в який гармонічно будуть імплементовані ключові європейські норми з чітким визначенням норм щодо свободи інформації та захистом персональних даних, а також деталізацією взаємодії та фіксацією відповідальності за порушення норм у сфері захисту персональних даних.

Література:

1. Єсімов С.С. Захист персональних даних у контексті розвитку динамічних систем. *Науковий вісник державного університету вну-*

тришніх справ. 2013. № 3. С.198–207. URL:http://www2.lvduvs.edu.ua/documents_pdf/visnyky/nvsy/03_2013/13yessdis.pdf.

2. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 року. URL: http://zakon3.rada.gov.ua/laws/show/994_326.

3. Про інформацію: Закон України від 13.01.2011 № 2657-XII. URL: <http://zakon5.rada.gov.ua/laws/show/265712>

4. «Про захист персональних даних» Закон України від 1.06.2010 року №2297-VI (зі змінами та доповненнями). URL: <http://zakon3.rada.gov.ua/laws/show/2297-17>.

5. Конституція України: Закон України 28 червня 1996 року №254к/96-ВР URL:<https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

Брайчевський С.М.

кандидат фізико-математичних наук,
старший науковий співробітник

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В СИСТЕМАХ ІНТЕРНЕТУ РЕЧЕЙ В УМОВАХ РЕЖИМНИХ ЗАХОДІВ

Швидкий розвиток сучасних інформаційних технологій породжує нові виклики і нові ризики, що потребують ретельного вивчення. До їх числа відносяться і проблеми правового регулювання, пов'язані з використанням Інтернету речей (далі – IP) [1-4]. Вони пов'язані з наявністю (принаймні, гіпотетичною) в поведінці систем IP елементів соціальної поведінки [2].

Ця поведінка сама по собі є складною і мало вивченою. В особливих соціальних умовах вона може набувати специфічних характеристик, що породжують якісно нові виклики і ризики. Такими умовами може бути, зокрема, запровадження режимних заходів.

Ключову роль відіграє та обставина, що функціонування кібернетичних систем здійснюється відповідно до алгоритмів, розроблених для визначених умов експлуатації. Режимні заходи тією чи іншою мірою передбачають зміну цих умов внаслідок перегляду низки правових норм. В результаті виникає можливість позаштатного функціонування окремих підсистем, коли конкретні задачі не можуть виконуватись в рамках наявних алгоритмів так, як це передбачалося розробниками системи. Це, в свою чергу, може призводити або до програмних збоїв, або до непередбачуваних результатів роботи системи. Аналогічні ситуації можуть виникати і в діяльності людини, але тоді зрозуміло, хто несе відповідальність, і яку саме, за можливі негативні наслідки. У випадку позаштатного функціонування кібернетичних систем це питання вирішити важко, оскільки розробники системи не передбачали можливість її експлуатації в змінених умовах, до того ж самі зміни не були заздалегідь відомі.

Однією з проблем, які активно обговорюються у зв'язку з розвитком IP, є захист персональних даних [5-8]. Причина полягає

перш за все в тому, що системи ІР за своєю природою призначені для збирання різноманітних даних, причому відповідно до певних алгоритмів, які не завжди відповідають загальноприйнятим нормам оперування конфіденційними відомостями. Важливо, що значна частина ризиків, що виникають, взагалі не пов'язані з штатними режимами експлуатації систем ІР. За певних умов, кібернетична система може оперувати даними, “не усвідомлюючи”, що вони означають чи можуть означати в суб'єктивному сприйнятті людиною. Машина використовує дані з певною метою, тоді як хтось може використати ці ж самі дані з іншою метою.

В роботі [9] нами були розглянуті ризики, пов'язані з обробкою персональних даних системами ІР з елементами штучного інтелекту. Подібні ризики можуть виникати і в простіших системах ІР (що не містять елементів штучного інтелекту) за рахунок зміни режиму їх експлуатації в умовах запровадження режимних заходів. Роль штучного інтелекту в таких випадках відіграє звичайний людський інтелект персоналу, який працює з персональними даними в нестандартних умовах. Специфічні дії персоналу, зумовлені характерними особливостями запроваджененого режиму, як такі не несуть в собі ніякої загрози (свідомі зловживання ми не розглядаємо). Але вони можуть змусити кібернетичну систему виконувати операції, що не передбачені в рамках її штатної експлуатації, і саме вони здатні породжувати певні ризики. Найгірше те, що ці ризики, як правило, є непрогнозованими. Саме тому персонал в подібних випадках не несе відповідальності за негативні наслідки, оскільки не порушує жодної норми.

Стосовно систем ІР для нас найбільший інтерес становлять ситуації, пов'язані з безпосереднім отриманням даних за допомогою датчиків та їх можливе несанкціоноване розповсюдження шляхом використання мережних технологій. Але мають бути розглянуті й складніші ситуації, зумовлені можливістю агрегування різних наборів даних (отриманих з різних джерел за допомогою різних технологій) в комплекси, придатні для якісно інших методів обробки. Так, наприклад, можуть формуватися набори персональних даних, які містять в собі значно більший обсяг інформації (в тому числі конфіденційної), ніж передбачено діючими нормами. Головний механізм полягає в тому, що машина може оперувати даними, які

вона самостійно збирає та опрацьовує в процесі вирішення задач, що виходять за межі лінійної обробки інформації, типової для “звичайних” кібернетичних систем.

Зазначимо, що на наш час саме поняття персональних даних знало певного розширення в порівнянні з традиційним розумінням їх як “паспортних даних”. Відповідно до Загального регламенту про захист даних (GDPR), діючого в межах законодавства Європейського Союзу щодо захисту персональних даних, це поняття визначається як “... будь-яка інформація, що стосується фізичної особи, яку ідентифіковано чи можна ідентифікувати” [10]. Аналогічно це поняття визначається і Законом України “Про захист персональних даних”. Тому процес агрегації різних даних, взагалі кажучи, може мати нетривіальні наслідки.

Нижче ми розглянемо один важливий аспект проблеми, який ґрунтується на автоматичній ідентифікації особи шляхом розпізнання образів.

Для нас важливими є такі моменти[10]:

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

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

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

З точки зору проектувальників, система ІР може взагалі не оперувати персональними даними, або оперувати ними в обмежених рамках. Але ми вже зазначили, що до персональних даних можуть бути віднесені будь-які відомості, так чи інакше пов'язані з тією чи іншою особою. І вони можуть складатися з кількох компонентів. Частину з них складають дані, передбачені штатним режимом експлуатації системи, в тому числі і дані, які мають опрацьовуватися персоналом, а частина - збирається і обробляється машиною.

Нехай відповідно до запроваджених режимних заходів система фіксує людину, поведінка якої має характерні риси, що зумовлюють необхідність опрацювання її даних, ідентифікує її за обличчям, а потім здійснює пошук в доступних базах для прийняття того чи іншого рішення. При цьому машина може завантажувати вміст баз даних, які містять дані на цю людину, створюючи її власний профіль. Оскільки такі дані машина використовує сама, ми можемо не мати про це жодного уявлення. Але за певних умов ці дані можуть бути кимось використані або відповідно до характеру роботи машини, або внаслідок зламу системи сторонніми особами.

Принциповим моментом є те, що тепер, після ідентифікації особи, будь-яка інформація стосовно неї потрапляє в категорію персональних даних, а отже вимагає захисту.

Такі ситуації породжують додаткові загрози в плані захисту персональних даних, важливість яких зумовлена в першу чергу тим, що машина фактично маніпулює наборами даних, склад і характер яких принципово не піддаються контролю.

Отже системи ІР за певних умов експлуатації, зумовлених запровадженням режимних заходів, в принципі здатні розширювати штатний режим збирання та обробки інформації, внаслідок чого машина отримує можливість оперувати персональними даними, використовуючи інші дані, отримані в передбачений спосіб. При цьому машина так чи інакше повинна використовувати додаткові дані, які вона збирає самостійно, використовуючи, наприклад, датчики різноманітних систем стеження.

В результаті виникають додаткові загрози в плані захисту персональних даних, важливість яких в першу чергу викликані принциповою неконтрольованістю наборів даних, якими фактично маніпулює

машина. Отже, виникає необхідність врахування таких загроз при розробці правових норм щодо захисту персональних даних, а також адекватних механізмів реалізації цих норм на практиці.

Список використаної літератури

1. Баранов А.А. Интернет вещей и искусственный интеллект: истоки проблемы правового регулирования - IT-право: проблемы та перспективи розвитку в Україні: збірник матеріалів II-ї Міжнародної науково-практичної конференції (Львів, 17 листопада 2017 р.). – Львів : НУ “Львівська політехніка”, 2017. – 318 с. (С. 18-42).

2. Рекомендации МСЭ-Т Y.2060 (06/2012). Серия Y: Глобальная информационная инфраструктура, аспекты протокола Интернет и сети последующих поколений. Сети последующих поколений - Структура и функциональные модели архитектуры. Обзор Интернета вещей. – Режим доступу: <http://handle.itu.int/11.1002/1000/11559>

3. Баранов О.А. “Интернет речей” як правовий термін.Юридична Україна. – 2016. – № 5-6. – С. 96-103. – Режим доступу: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/urykr_2016_5-6_16.pdf

4. Черняк Л. Платформа Интернета вещей (рус.). Открытые системы. СУБД, №7, 2012. Открытые системы. URL: <https://www.osp.ru/os/2012/07/13017643/>

5. Баранов О.А., Брижко В.М. Захист персональних даних в сфері інтернет речей. “Інформація і право” – 2016 – № 2(17)/ – С. 85-91
Режим доступу: http://ippi.org.ua/sites/default/files/11_0.pdf

6. Становлення і розвиток правових основ та системи захисту персональних даних в Україні : монографія / В.Г. Пилипчук, В.М. Брижко та ін. ; за ред. В.М. Брижка, В.Г. Пилипчука.- Київ: ТОВ “Видавничий дім “АртЕк”, 2017.- 226 с.

7. Интернет вещей: чем угрожает будущее. –Режим доступу: <http://igate.com.ua/news/3169-internet-veshhej-chem-ugrozhaet-budushhee>

8. Как в 2015 году был взломан Интернет вещей. –Режим доступу: <http://igate.com.ua/news/12342-kak-v-2015-godu-by-l-vzloman-internet-veshhej>

9. Брайчевський С. М. Проблема персональних даних в системах Інтернету речей з елементами штучного інтелекту. “Інформація і право” – 2019 – №4(31)– С. 61-67 – Режим доступу : <http://ippi.org.ua/braichevskii-sm-problema-personalnikh-danikh-v-sistemakh-internetu-rechei-z-elementami-shtuchnogo-in>

10. Загальний регламент про захист даних (GDPR)– Режим доступу: <https://gdpr-text.com/?col=2&lang1=ukr&lang2=en&lang3=ru> main

Дранник В.А.

викладач кафедри філософії ФСП
КПІ ім. Ігоря Сікорського

ПРОБЛЕМА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ГРОМАДЯН

Сьогодні дедалі гострішою стає проблема захисту інформаційної приватності та персональних даних громадян України. Захист персональних даних своїх громадян та забезпечення їх інформаційної приватності повинно бути одним із головних пріоритетів будь-якої правової держави.

В цій сфері основоположним є Закон України «Про захист персональних даних». В законі розглядаються наступні положення: поняття про персональні дані, суб'єкти персональних даних та їх права, підстави для обробки персональних даних, відповідальність за порушення законодавства про захист персональних даних тощо.

Потужний розвиток цифрових технологій та інформаційної сфери може нести в собі небезпеку щодо витоку інформації особистих персональних даних. Але, в багатьох випадках громадянин повинен передавати свої персональні дані, інакше без цього він не отримає те, заради чого він звертається до установи. Сьогодні, куди б людина не звернулася, вона повинна заповнювати папери і надавати особисту інформацію: паспортні дані, адреса, номер телефону, а подекуди і, навіть, особисте фото. Коли громадянин надає згоду на обробку персональних даних, то він не знає де надалі ці дані будуть поширюватися, де і як будуть зберігатися, чи будуть вони знищені, і хто взагалі має доступ до цих даних. А найважливіше, чи будуть передаватися ці персональні дані третім особам і подальша законність їх використання.

Повинна бути правова відповідальність за порушення або розголошення третім особам конфіденційної особистої інформації. Держава мусить забезпечувати не тільки на законодавчому рівні, а й фактично захищати громадян від незаконної обробки їх персональних даних. Кожна людина бажає відчувати інформаційну безпеку та захист особистих даних.

Існує нагальна потреба у створенні діючого вузькопрофільного органу, який буде регулювати питання захисту персональних даних та персональної інформації, яку громадяни України оприлюднюють згідно вимог законодавства. Також, цей орган повинен контролювати дотримання законності щодо збору, обробки, використання, зберігання особистої інформації громадян та захищати від незаконної обробки цієї інформації, накладати санкції правопорушникам і слідкувати за їх виконанням.

Також, для забезпечення захисту особи від незаконного доступу, обробки, розповсюдження персональної інформації, дуже важливо:

- насправді виконувати норми Закону України «Про захист персональних даних»;
- здійснювати кримінальне покарання за незаконний доступ та незаконне розповсюдження персональних даних громадян;
- захищати права і забезпечувати безпеку людини в умовах цифрових перетворень та інформаційній сфері тощо;
- адаптувати законодавства України з питань захисту прав і безпеки людини в інформаційній сфері до законодавства ЄС.

Таким чином, однією із сучасних небезпек для людини є незаконне розповсюдження її приватної інформації. Важливо ухвалити зміни до законодавства задля мінімізування витоку персональних даних.

Подальші напрями розвитку цієї теми можуть бути направлені на розробку, вдосконалення, впровадження та дотримання нових ефективних доповнень (змін) до Закону України «Про захист персональних даних».

Уханова Н.С.

старший науковий співробітник
НДІП НАПрН України

ЗАРУБІЖНИЙ ТА ВІТЧИЗНЯНИЙ ДОСВІД ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ У СФЕРІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

Сучасний розвиток інформаційних технологій у різних сферах впливає на зміну не лише способів взаємодії між окремими індивідами, але і визначає нові детермінанти для формування передумов виникнення нових підходів до організації суспільних відносин. Розвиток інформаційно-комунікаційних технологій створює не лише значні переваги, але і суттєві ризики, пов'язані з неконтрольованим доступом до інформації. Досить актуальною проблемою у цьому аспекті є захист персональних даних, як особливий предмет інформаційної взаємодії. Зважаючи на відносно нетривалу історію розвитку інформаційного суспільства та стрімкий розвиток нових форм обміну даними, врегулювання правових аспектів інформаційних відносин завжди залишається важливим завданням.

Забезпечення захисту персональних даних в інформаційному суспільстві передбачає вирішення численного ряду питань, пов'язаних із дотриманням достатнього рівня приватності життя індивідів. Захист персональних даних є складовою системи інформаційної безпеки, що дозволяє забезпечити особисту безпеку, баланс інтересів особистості, суспільства та держави у сфері обробки інформації [4].

Правові аспекти захисту персональних даних, зважаючи на інтернаціональний характер міжнародного інформаційного обміну, регулюються в значній мірі міжнародними нормативними актами [7]. Важливу увагу слід звернути на законодавство Європейського Союзу, яке акумулювало правові механізми захисту різних типів персональних даних.

Рекомендація № R(87)15 Комітету Міністрів Ради Європи регулює окремі питання щодо використання персональних даних публічними органами державної влади [5]. Ключові принципи

наведеної Рекомендації передбачають доведення факту легітимності використання відповідних персональних даних публічними органами влади, які здійснюють опрацювання інформації стосовно окремих індивідів. Рекомендація визначає певне групування критеріїв віднесення чутливої інформації до загальнодоступних і спеціальних. Відповідно до даного нормативного документу, обробка інформації про індивіда, яка може відноситися до расової, національної приналежності, політичних поглядів, релігійних або філософських переконань, стану здоров'я, інтимного життя, не повинна допускатися без спеціального дозволу. Відомості, що характеризують фізіологічні та біологічні особливості людини, на підставі яких можна встановити її особистість (особиста інформація) і які використовуються компетентними органами для встановлення статусу індивіда, можуть оброблятися лише за наявності письмової згоди фізичної особи, окрім деяких окремих випадків. Обмін персональними даними про індивідів між окремими організаціями, які функціонують на території різних держав, які є сторонами Конвенції Ради Європи 108 і може бути заборонена або обмежена в цілях інформаційного захисту. Конвенція No108 у главі II, яка називається «Основні принципи захисту даних» вказує, зокрема, на необхідність створення в країнах-учасниках особливого режиму правового захисту «чутливих даних» [1].

Регламент 2016/679 Європейського парламенту і Ради від 27 квітня 2016 року «Про захист фізичних осіб стосовно обробки персональних даних та про вільне переміщення таких даних, а також про скасування Директиви 95/46/ЄС», визначає певні обмеження для використання персональних даних в окремих процесах суспільного життя [3]. Даний нормативний документ досить чітко розмежовує зміст різних категорій персональних даних та дозволені умови їх використання і розголошення. Важливий аспект у нормативному акті відведено збереженню приватності та можливості використання певної чутливої інформації третіми особами [10]. Так, відповідно до п. 50 Регламенту 2016/679 обробка персональних даних в інших цілях, ніж ті, для яких персональні дані були спочатку зібрані, має бути дозволена тільки там, де обробка сумісна з визначеним колом завдань, які мають бути підтверджені відповід-

ними компетентними органами. Варто відмітити, що важливість даного положення впливає з наявного негативного історичного досвіду міжнародних скандалів, пов'язаних з розголошенням особистої конфіденційної інформації індивідів. Зокрема, як приклад, можна навести скандал з Wikileaks (2010 р.), в рамках якого відбулося розголошення у мережі Інтернет листування дипломатичного відомства США. У 2013 Едвардом Сноуденом, експрацівником Агентства національної безпеки США, через Інтернет було розголошено факти про роботи американських та британських спецслужб. Досить гучними можна назвати наслідки скандалу з «Cambridge Analytica», яка надала доступ до інформації про 50 млн. користувачів мережі «Facebook», що вплинуло на результати виборів президента США у 2016 році [6].

Розглядаючи правові аспекти регулювання питання захисту персональних даних в Україні, варто відмітити, що розвиток вітчизняного законодавства в даній сфері у значній мірі зорієнтований на наслідування європейської юридичної практики. З 2011-го року набрав чинності Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI [8], який визначає загальне правове підґрунтя для формування інформаційних взаємодій з використання чутливих (персональних) даних, їх обробкою та забезпечення належного захисту. У ст. 6 даного нормативного документу визначено основні вимоги, які поставлено перед процесами обробки персональних даних. Наведемо особисте трактування визначених законодавством вимог, з урахуванням певного практичного досвіду реалізації положень вітчизняного законодавства у сфері захисту персональних даних [9]:

- чітке визначення мети для обробки персональних даних та наявність правового обґрунтування підстав, що передбачають провадження процедури обробки відповідної інформації;
- вимоги достовірності до персональних даних передбачають необхідність їх періодичного оновлення, яка визначається специфікою тих процесів інформаційного обміну, в рамках яких відповідні персональні дані використовуються;
- до категорії персональних даних відносяться відомості про фізичну особу, які мають бути підтверджені документально;

- цілі та завдання використання персональних даних мають визначатися конкретними випадками, які визначено законодавчо;
- для початку обробки персональних даних обов'язковим є отримання згоди від фізичної особи у визначеному законодавством порядку;
- законом визначаються можливості для введення обмежень на обробку персональних даних, зокрема коли мова йде про порушення добробуту індивіда, засад національної безпеки, тощо;
- важливим критерієм обробки персональних даних є обов'язкова ідентифікація фізичної особи, але в міру визначених на законодавчих підставах цілей.

Іншим важливим документом, що регулює правові засади обробки персональних даних в Україні, є Закон України «Про доступ до публічної інформації» від 13.01.2011 № 2939-VI [9]. Даним нормативним документом визначено вимоги до знеособлення персональних даних, обов'язкової згоди з боку індивідів на розкриття та поширення персональної інформації про них, визначення ряду обмеження щодо доступу до відповідної персональної інформації, тощо. Прийняття даного закону дало можливість уникнути ряду правових колізій, які виникали раніше у сфері правового захисту персональних даних, зокрема відсутності чіткого розмежування публічної (загальнодоступної) та персональної інформації.

Не зважаючи на певні позитивні кроки у розвитку вітчизняного законодавства у сфері захисту персональних даних, все ж таки воно потребує подальшого доопрацювання та внесення відповідних змін, які продиктовані вимогами часу. Основними проблемами, які залишаються нині в Україні у сфері обробки персональних даних, можна визначити наступні [5]:

- недосконалість механізмів правового захисту у процесі збору та передачі персональної інформації;
- порушення строків обробки персональної інформації;
- відсутність правового регламентування ряду питань у сфері обробки персональних даних з використанням сучасних веб-платформ та соціальних мереж;
- нечіткість механізмів захисту щодо нерозголошення персональної інформації з боку співробітників відповідних організацій, що працюють з персональними даними;

– відсутність механізмів правового врегулювання ситуацій з втрати або пошкодження персональних даних, їх несанкціонованого витоку.

В сучасних умовах діяльність багатьох підприємств та організацій у сфері обслуговування фізичних осіб (надання різноманітних сервісних послуг у сферах логістики, зв'язку, туризму, тощо) передбачає обов'язкове надання персональної інформації. Проте, досить часто, така практика суперечить базовим законодавчим вимогам щодо прав людини на приватність особистого життя. Це пояснюється тим, що у випадку незгоди на обробку персональної інформації, людині може бути надано відмову у наданні певних послуг. На наш погляд, така ситуація також потребує невідкладного правового врегулювання.

Таким чином, правові аспекти захисту персональних даних на сьогодні є досить важливими для підтримання належного рівня безпеки у сфері інформаційного обміну. Розвиток вітчизняного законодавства у сфері захисту персональних даних у значній мірі зорієнтований на наслідування європейської юридичної практики. Наявна зарубіжна та вітчизняна правова база регулює багато питань, пов'язаних з захистом персональних даних. Однак, існує певний перелік проблем законодавчої невизначеності у сфері доступу та забезпечення конфіденційності персональної інформації. Вирішенню цих проблем має передувати ґрунтовне опрацювання на законодавчому рівні сучасних тенденцій у зміні технологій обробки інформації та її поширення, врахування особливостей та методів забезпечення конфіденційності чутливої інформації.

Список використаних джерел

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних Міжнародний документ від 28.01.1981 р. URL: http://zakon3.rada.gov.ua/laws/show/994_326.
2. Рекомендація № R(87)15 Комітету Міністрів державам-членам, що регулює використання персональних даних у секторі поліції від 17 вересня 1987 року. URL: http://cyberpeace.org.ua/files/rekomendacia_km_radi_evropi_sodo_vikoristanna_personal_nih_danih_sektori_policii.pdf

3. Положення (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб стосовно обробки персональних даних та щодо вільного переміщення таких даних та скасування Директиви 95/46 / ЄС (Загальні положення про захист даних) URL: <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.

4. Гуйван О.П. Охорона персональних даних як потреба демократичного суспільства // Цивільне прав і процес. 2018. №4. С. 34-40

5. Гронь О. В., Погореленко А. К. Проблеми захисту персональних даних у контексті сучасної комунікації. Науковий вісник Ужгородського національного університету. Серія : Міжнародні економічні відносини та світове господарство. 2018. №19(1).С. 102-108

6. Мітрухов П.М. Шляхи вирішення окремих правових проблем щодо захисту персональних даних. Актуальні питання протидії кіберзлочинності та торгівлі людьми : збірник матеріалів Всеукр. наук.-практ. конф. (23 листопада 2018 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЕ в Україні. Харків : ХНУВС, 2018. с. 62-66

7. Куценко Р.В. Поняття та склад персональних даних працівників за трудовим законодавством України. Науковий вісник публічного та приватного права. 2017. № 2. С. 78-82.

8. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI [електронний ресурс] – режим доступу: <https://zakon.rada.gov.ua/laws/show/2297-17>

9. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI URL: <https://zakon.rada.gov.ua/laws/show/2939-17>

10. EU General Data Protection Regulation (GDPR). URL: <http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf>.

Вальчук О.І.

кандидат історичних наук, асистент
кафедри правових наук та філософії,
Вінницький державний
педагогічний університет
імені М. Коцюбинського

Петрик В.В.

здобувач СВО магістра, Вінницький
державний педагогічний універси-
тет імені М. Коцюбинського

**ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ
ПЕРСОНАЛЬНИХ ДАНИХ ПРАЦІВНИКІВ АПАРАТУ
ДЕРЖАВНОЇ СЛУЖБИ УКРАЇНИ
З НАДЗВИЧАЙНИХ СИТУАЦІЙ**

Зміна парадигми представлення інформації, повсюдна діджиталізація вимагають відповідного рівня нормативно-правового забезпечення та цифрової культури. Не менш важливою є проблема захисту інформаційної приватності та персональних даних громадян. Чинний нині Закон України «Про захист персональних даних» був прийнятий Верховною Радою України 01 червня 2010 р. [1]. Він регулює правові відносини, що пов'язані з обробкою персональних даних і захистом конституційного права на невтручання в особисте життя. Необхідні заходи щодо його реалізації проводяться у всіх державних органах.

Державна служба України з надзвичайних ситуацій (далі – ДСНС України) не залишається осторонь від означених процесів. У цій сфері у межах діяльності усіх структурних підрозділів були визначені наступні основні напрямки: розробка типових положень про порядок обробки персональних даних; підготовка та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, у яких обробляються персональні дані; модернізація інформаційно-телекомунікаційних систем, призначених для обробки персональних даних. Зауважимо, що юристи апарату ДСНС України беруть активну участь у семінарах

та обговореннях, щодо питань захисту персональних даних. Такі заходи дають можливість учасникам поділитися власним досвідом, почути думку інших фахівців, і власне отримати позитивний досвід [2].

З метою удосконалення порядку обробки персональних даних, що є власністю держави, в інформаційних системах апарату ДСНС України, на виконання Законів України «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних» та постанови Кабінету Міністрів України від 29 березня 2006 р. № 373 «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» спеціальним наказом Державної служби України з надзвичайних ситуацій від 02 липня 2013 р. №439 начальнику Управління телекомунікацій, інформаційних технологій та Системи 112 Лоєнку А.О. було доручено організувати, а начальнику центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій ДСНС України Гайдаю О.В. – провести роботи щодо розроблення та впровадження комплексної системи захисту інформації в інформаційно-телекомунікаційних системах, у яких обробляються персональні дані в Департаменті економіки та фінансів, та 3-х комплексних систем захисту інформації в інформаційних системах, у яких обробляються персональні дані в Департаменті персоналу [3].

Поступово означені заходи здійснюються і в структурних підрозділах. Наприклад, у 2017 р. з метою модернізації інформаційно-телекомунікаційних систем, призначених для обробки персональних даних Головного управління ДСНС України у Вінницькій області відповідним наказом було створено комплексні системи захисту інформації в інформаційно-телекомунікаційних системах відділу економіки та фінансів та відділу персоналу та призначено позаштатну службу захисту інформації. Керівником служби було визначено – заступника начальника центру оперативного зв'язку, системним адміністратором – заступника відділу інформаційних технологій центру оперативного зв'язку, телекомунікаційних систем та інформаційних технологій, адміністратором безпеки – провідного фахівця відділу інформаційних технологій центру

оперативного зв'язку, телекомунікаційних систем та інформаційних технологій [4]. Цього ж року відповідальною особою за звітність, обробку та збереження бази персональних даних співробітників Головного управління призначили начальника відділу персоналу.

Важливим є також питання закріплення єдиних узагальнених стандартів етичної поведінки осіб, які мають доступ до персональних даних. Наказом Міністерства внутрішніх справ України від 16 листопада 2018 р. №932 було затверджено Правила етичної поведінки працівників Державної служби України з надзвичайних ситуацій, територіальних органів, підприємств, установ та організацій, що належать до сфери її управління. Відповідно до означеного нормативно-правового акту, працівникам ДСНС забороняється розголошувати персональні дані фізичних осіб, конфіденційну та іншу інформацію з обмеженим доступом, режим якої встановлено Законами України «Про державну таємницю», «Про інформацію», «Про захист персональних даних» та «Про доступ до публічної інформації», що стали їм відомі у зв'язку з виконанням посадових обов'язків. Якщо працівникам ДСНС стало відомо про загрозу чи факти неправомірного поширення інформації з обмеженим доступом, вони повинні негайно повідомити про це безпосереднього керівника [5].

Таким чином, процеси цифровізації традиційного інформаційного середовища нерозривно пов'язані з потребою належного забезпечення прав, свобод і безпеки людини. Захист персональних даних є одним із важливих напрямків у цій сфері. Необхідні заходи здійснюються у всіх органах державної влади, в тому числі й в апараті, територіальних органах та підрозділах ДСНС України. Важливим є забезпечення швидкості реагування на зміни у сучасному світі та відповідності існуючих норм та стандартів до потреб суспільства.

Список використаної літератури

1. Про захист персональних даних. Закон України від 01.06.2010 № 2297-VI. Редакція від 20.03.2020 URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 13.05.2020).

2. ГУ ДСНС України у Харківській області. Юристи Головного управління ДСНС України у Харківській області взяли участь у семінарі щодо захисту персональних даних. URL: <https://kh.dsns.gov.ua/ua/Ostanni-novini/11265.html> (дата звернення: 13.05.2020).

3. Про розроблення та впровадження комплексних систем захисту інформації в інформаційно-телекомунікаційних системах апарату ДСНС України. Наказ Державної служби України з надзвичайних ситуацій від 02.07.2013 р. №439. URL: <https://www.dsns.gov.ua/files/2013/11/25/439.pdf> (дата звернення: 15.05.2020).

4. Про створення КСЗІ в інформаційно-телекомунікаційній системах, призначених для обробки персональних даних ГУ ДСНС України у Вінницькій області. Наказ ГУ ДСНС України у Вінницькій області від 21.02.2017 р. №71. URL: <https://vn.dsns.gov.ua/ua/Nakazi-z-osnovnoyi-diyalnosti/6961.html> (дата звернення: 15.05.2020).

5. Правила етичної поведінки працівників Державної служби України з надзвичайних ситуацій, територіальних органів, підприємств, установ та організацій, що належать до сфери її управління. URL: <https://zakon.rada.gov.ua/laws/show/z1376-18> (дата звернення: 16.05.2020).

Julia V. Strebkova

Ph.D. (Philosophy), docent.

REVIEW OF BIOPOLITICS NORMS IN ADJUSTMENT OF REPRODUCTION IN UKRAINE

Statement of the Problem. Women are vulnerable group in reproductive pressure and intersection discrimination in Ukraine. The dependence of women on their intimate partners is increasing. Discriminatory bills are constantly in the parliament. Unscientific and fake publications in bioethics field escalate into a scandal.

Solving of these problems in scientific methods is complicated. There is clericalism inside Ukrainian social sciences and the strong influence of religious organizations on legislative and executive power. The religious leaders have been strong opposes the ratification of the Istanbul Convention. We note, that religious organizations often have external information and financial sources. Former Chief of Foreign Intelligence Service of Ukraine Ye. Bozhko in an interview to platform Ukrinform noted that „The Russian Orthodox Church is 99% controlled by the secret services of the Russian Federation” [4].

The situation in biopolitics is complicated by the fact that anti-gender information projects are part of Russia’s hybrid informational war against Ukraine. And this requires powerful, worthy counteraction. Currently, the site of Personal Information Security is working [6], and different aspects of information sovereignty of the country have been researching. V. Iierusalymov in the work „Hybrid gender threats as an element of destabilization of the Verkhovna Rada of Ukraine”, with referring to recently discovered data from Russian security agencies, designate that “among other things, information on the ROC’s close cooperation with the Russian authorities have been provided” [5]. But, in general, Gender aspects of information security are insufficiently developed, in particular in the field of biopolitics and reproduction.

Methodology. Social context of legal norms of the last 5 years, which determine the national biopolitics in the regulation of reproduction, have been analyzed.

Conclusion & Significance. In Ukraine theology is a scientific branch, but gender studies are not included in this list. Such an approach does not

contribute to solving women's problems. Now in Ukraine there is a closed circle of negative reproduction: a woman has no means for contraception, then she has no means for abortion - does not have the means for keeping the child - increasing dependence on the intimate partner - a new unwanted pregnancy. At each link in this way, there is a legislative regulation with different efficiency, but it does not provide out of this circle. The weakest link in this process is the transition from unwanted pregnancy to the birth of an unwanted child. As result: illegal abortions, abuse of children, significant number of infanticide - criminal implementation under Paragraph 117 of the Criminal Code. To effectively solve this social problem, it is necessary to find out who was the child's father.

The Order of the Ministry of Health approved the Procedure for the use of assisted reproductive technologies in Ukraine and the Procedure for referring women for the first course of infertility treatment by methods of assisted reproductive technologies in absolute terms for the budget (2019 year). This is important because in the world community Ukraine and Russia are centers for commercial international surrogacy arrangements, which create "otherguess set of cross-border relationships."

It is worrying that moral and ethical norms in biopolitics are currently under religious cap, and the massive ecclesiastical influence of the ROC "consolidates social boundaries in the paradigm of policy of the Russian Federation"[5]. The Russian Orthodox Church in its „Foundations of a Social Concept" since 2000 calls surrogacy „unnatural and morally unacceptable", regardless of whether it is done for money or on a non-profit basis [7]. Representatives of the ROC, in particular, head of Department for External Church Relations of the Moscow Patriarchate (DECR) still confirm this position even now [3].

Regarding the current norms of Ukrainian law, consent of the surrogate mother's husband to participate in the surrogacy program is provided, which requires further gender analysis of different reproductive rights and opportunities for women of different matrimonial status. The issue of the application of assisted reproductive technologies also has a financial dimension. The paternity test is currently not well regulated and is not available at costliness for majority of Ukrainian women.

There are positive trends: punishment of alimony debtors. Realization of this law is also depend on effective paternity tests. To effectively

solve these social problems, paternity test is necessary to make legally admissible and available for different groups of women.

The Regulation on the State Center for Family Planning and Reproductive Health, in addition to providing access to contraception, provides development of information materials for young people on safe sexual behavior, healthy lifestyles, responsible parenthood. At the same time, the Ministry of Education and Science of Ukraine recently returned the subject “Family basics” to schools. The methodological materials for this course present contraceptives as an absolute evil, and the textbook in general is an example of anti-scientific approaches to the problems of biopolitics. As a result, the younger generation of women may have difficulty exercising their sexual and reproductive rights.

Thus, solving the problem of protection of human rights and safety of women in the field of reproduction involves overcoming the religious information influence of the Russian Federation on the legislative and executive authorities of Ukraine.

References

1. A study of legal parentage and the issues arising from international surrogacy arrangements. Preliminary Document No 3 C of March 2014 for the attention of the Council of April 2014 on General Affairs and Policy of the Conference. <https://assets.hcch.net/docs/bb90cfd2-a66a-4fe4-a05b-55f33b009cfc.pdf>

2. Report of the Special Rapporteur on the sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material. Human Rights Council. Thirty-seventh session 26 February–23 March 2018. Agenda item 3. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

3. Глава отдела внешних церковных связей Московского патриархата митрополит Волоколамский Иларион. Интервью РИА Новости. URL: <https://webcache.googleusercontent.com/search?q=cache:9qhwV1oZfhsJ:https://ria.ru/20191206/1562037765.html+&cd=2&hl=uk&ct=clnk&gl=ua&client=firefox-b-d> (дата звернення: 26.02. 2020).

4. Божок Євген. Інтерв'ю Українському національному інформаційному агентству «Укрінформ». URL: <https://www.ukrinform.com>

ua/rubric-society/2626340-rosijska-pravoslavna-cerkva-na-99-pid-kontrolom-fsb-golova-rozvidki.html (дата звернення: 25.04. 2020).

5. Ієрусалимов Владислав Ігорович. Гібридні гендерні загрози як елемент дестабілізації діяльності верховної ради України. http://academy.ssu.gov.ua/ua/page/page_1581345413.htm (дата звернення: 20.04. 2020).

6. Інформаційна безпека особистості: веб-сайт. URL: <https://sites.google.com/site/infobezpekaosobu/informacijna-bezpeka> (дата звернення: 20.04. 2020).

7. Основи Соціальної концепції Руської Православної Церкви // Офіційний сайт Московського патріархату. URL: <http://www.patriarchia.ru/ua/db/text/1207692.html> (дата звернення: 20.04. 2020).

8. Порядок застосування допоміжних репродуктивних технологій в Україні. URL: <https://zakon.rada.gov.ua/laws/show/z1697-13> (дата звернення: 20.04. 2020).

Грищук А.Б.

кандидат юридичних наук,
доцент кафедри адміністративно-правових дисциплін, юридичного факультету Львівського державного університету
внутрішніх справ

ІНФОРМАЦІЙНО-ПРАВОВІ СКЛАДОВІ ІНТЕГРУВАННЯ КУРСІВ ЕЛЕКТРОННОГО НАВЧАННЯ У НАВЧАЛЬНИЙ ПРОЦЕС ПРОФЕСІЙНОЇ ПІДГОТОВКИ ДЕРЖАВНИХ СЛУЖБОВЦІВ В УКРАЇНІ

Важливі проблеми, що виникають за впровадження інформаційно-комунікаційних технологій в освітню сферу за умов формування та розвитку інформаційного суспільства, стосуються якості управління персоналом навчальних закладів, зокрема науковими та викладацькими кадрами.

Під час створення курсу електронного навчання важливо зважати на особливості цільової групи, для якої призначений цей курс, і вибір методики дистанційного навчання з урахуванням характеристик технічного забезпечення. Відтак існує ціла низка аспектів інформатизації освіти.

Зокрема, з'явився новий термін «візуальна освіта», який означає, що у навчанні зображення, образ, моделі, знаки виконуватимуть усе більшу роль, витісняючи звичні тексти. Робота зі знаками і знаковими системами, перехід із однієї знакової системи в іншу, кодування та декодування – навиками таких процесів повинна володіти людина інформаційного суспільства. Відтак постає питання про інформаційну культуру особистості, під якою розуміють наявність знань у галузі інформації та вміння працювати з інформацією.

Інформаційна культура особистості, вважають учені, потребує постійного формування. Тому в другій половині ХХ ст. виникає напрям медіа-освіти, яка досліджує питання про вивчення державними службовцями засобів масової комунікації. Основні завдання медіа-освіти полягають у: підготовці державних службовців до

діяльності в умовах інформаційного суспільства; формуванні у них умінь користуватися інформацією різних видів; володінні способами спілкування за допомогою інформаційних технологій і засобів, тобто здійсненні комунікації; усвідомленні наслідків впливу на людину засобів інформації, зокрема засобів масової комунікації [1]. У системі підготовки державних службовців розвинених країн вивчається спеціальний предмет, спрямований на вирішення цих завдань, що охоплює поняття про комунікації, знакові системи, подання інформації, засоби масової комунікації, концепції розвитку інформаційних технологій і систем, системи розподільної обробки даних, технології мультимедіа, інтелектуальні інформаційні технології [2, с. 4].

Основною метою впровадження цього освітнього продукту є забезпечення кваліфікованої практичної підготовки державних службовців до роботи як учасників державного замовлення – потенційних сумлінних виконавців державного замовлення.

На думку У. Хортон К. Хортон, нові інформаційні технології в освіті охоплюють три складові: технічні пристрої, програмне забезпечення та навчальне забезпечення [3, с. 12]. До сучасних технічних пристроїв, окрім комп'ютера, належать принтер, сканер, телевізійна й відеоапаратура, пристрої для перетворення інформації з однієї форми в іншу тощо. Оскільки комп'ютер є основою інформаційних технологій, зазвичай інформатизацію освіти розуміють як комп'ютеризацію навчання, тобто використання комп'ютера як засобу навчання і ширше – як багатоцільове використання комп'ютера у навчальному процесі.

Другою складовою інформаційних технологій є програми, що керують роботою на комп'ютері й обслуговують цю роботу.

На думку М. Меллінга, третю, найголовнішу, складову інформаційних технологій становить навчальне забезпечення як особливий клас програм – навчальні програми, навчальні системи [4, с. 21–24]. Власне вони і визначають процес і технологію комп'ютерного навчання, а також постійно удосконалюються фахівцями.

За визначенням учених, інформатизація освіти спричиняє істотні зміни багатьох аспектів навчального процесу [5]. Змінюється діяльність викладача й особи, яка навчається. Особа, яка навча-

ється, може оперувати значним обсягом різноманітної інформації, інтегрувати її, має змогу автоматизувати її обробку, моделювати процеси і вирішувати проблеми, бути самостійною у навчальних діях тощо. Викладач також звільняється від рутинних операцій, отримує змогу діагностувати осіб, які навчаються, відстежувати динаміку їх навчання і розвитку. Водночас, на думку учасників науково-практичної конференції «Інноваційні комп'ютерні технології у вищій школі», деякі викладачі не готові до переходу від аудиторної форми навчання, зокрема традиційного навчання, до використання інформаційних технологій в освіті [6]. Електронна техніка наразі використовується здебільшого як допоміжний засіб навчання. Певною мірою комп'ютер і нові інформаційні технології поступово поглинати процес, але, очевидно, не замінять повністю традиційні технології навчання.

За наявності систем управління освітою, які жорстко контролюють умови організації та процес навчання, ігнорування особливостей дистанційних освітніх технологій призводить до демотивації установ освіти щодо використання дистанційних освітніх технологій і загалом до уповільнення темпів розвитку дистанційних освітніх технологій в Україні.

Зокрема, згідно з чинним законодавством установи освіти, які реалізують електронне навчання, у ліцензійних нормах зазвичай вказують чисельність територій, де навчатиметься визначена кількість осіб. Вимоги до бібліотек такого вишу не враховують індивідуальні комплекти навчально-методичних матеріалів для осіб, які навчаються, і ресурси Інтернет-бібліотеки.

На основі досвіду діяльності закладів освіти, що в повному обсязі застосовують дистанційні освітні технології (наприклад, у Польщі), доцільно розробити специфічні вимоги для ліцензування закладів освіти, що відображають особливості дистанційного навчання. Сутність запропонованих змін ліцензійних нормативів заснована на доведенні факту еквівалентності багатьох видів програм навчання у традиційних формах і електронного навчання (слід враховувати специфіку навчання за програмами загальної підготовки державних службовців і програмами навчання за напрямами державного управління у різних сферах виконавчої влади).

На мою думку, основні вимоги до установ електронної освіти у системі професійної підготовки державних службовців доцільно передбачити у положеннях «Про Ліцензійних умов провадження освітньої діяльності», «Про акредитацію вищих навчальних закладів і спеціальностей у вищих навчальних закладах та вищих професійних училищах» з урахуванням вимог, що висуваються до установ дистанційної освіти. Законодавчо слід закріпити додаткові вимоги:

- пропускна здатність телекомунікаційного каналу установ, що використовують технології електронного навчання, має бути достатня для організації навчального процесу за всіма видами навчальної роботи і технологіям педагогічного спілкування, передбаченим навчальним планом і календарним графіком інформаційне забезпечення навчального процесу;

- освітньої діяльності мають становити інформаційні ресурси на різних носіях і засоби оперативного доступу до них;

- інформаційні ресурси мають повною мірою забезпечувати навчальний процес;

- професорсько-викладацький склад, інженерно-технічний та навчально-допоміжний персонал повинні періодично проходити перепідготовку або підвищення кваліфікації у галузі нових інформаційних та освітніх технологій;

- установи, що використовують технології електронного навчання, повинні мати сертифікованих фахівців у галузі управління комп'ютерними мережами та базами даних.

Адаптація українського законодавства до стандартів ЄС, завершення політичних й економічних реформ, вироблення скоординованої державної політики тощо вимагають значного фінансування, якого недостатньо у розпорядженні уряду України. Європейська Комісія підтримує країни-партнери Європейської політики сусідства та надає технічну допомогу через інструменти, що вже підтвердили свою ефективність у країнах із перехідною економікою (нові держави-члени ЄС): через цільову експертну допомогу (Технічна допомога та інформаційний обмін TAIEX), довготермінові твінінгові проекти, секторальну бюджетну підтримку, яка дозволяє дофінансувати з бюджету ЄС національні програми реформування певних секторів економіки. В Україні, на відміну від країн Центральної Європи, де

інструменти міжнародної технічної допомоги довели свою ефективність, вищезазначені інструменти використовуються неефективно, не беруться до уваги їх значущість та корисність, практичні рекомендації експертів реалізуються частково [7].

У сучасному інформаційному суспільстві основою розвитку цивілізації є інформаційні процеси, зокрема широке застосування мають інформаційно-комунікаційні технології. Впровадження інформаційно-комунікаційних технологій у сфері діяльності людини сприяло виникненню і розвитку глобального процесу інформатизації. Своєю чергою, цей процес сприяв розвитку інформатизації освіти, що є однією з найважливіших умов реформування та модернізації системи вітчизняної освіти у сфері державної служби.

У контексті приєднання України до Болонського процесу вітчизняна система освіти зазнала перегляду. Останніми роками тенденція тягнє до інтеграції України до європейського освітнього простору, а отже, її реформування. Доцільно відтак зазначає Г. Калінічева, що одним із головних напрямів реформування вітчизняної освіти є його інформатизація [8, с. 66–67], яка на сучасному етапі розвивається за чотирма основними напрямками:

- оснащення освітніх установ сучасними засобами інформатики та використання їх як нового педагогічного інструменту, який дає змогу істотно підвищити ефективність освітнього процесу. Цей напрям одержав в нашій країні назву педагогічної інформатики. Розпочавшись з освоєння і фрагментарного впровадження новітніх інформаційних технологій у традиційні навчальні дисципліни, педагогічна інформатика стала розвивати і пропонувати педагогам нові методи й організаційні форми навчальної роботи, які в подальшому стали використовуватися повсюдно і сьогодні здатні підтримувати практично все різноманіття освітнього процесу у системі вищої освіти. Проблема тут полягає лише у рівні оснащеності освітніх установ сучасними засобами інформатизації;

- використання сучасних засобів інформатики, інформаційних телекомунікацій і баз даних для інформаційної підтримки освітнього процесу, забезпечення можливості віддаленого доступу педагогів і осіб, які навчаються до наукової та навчально-методичної інформації і у своїй країні, і в інших країнах світового співтовариства;

– розвиток і поширення дистанційної освіти – нового методу реалізації процесів освіти та самоосвіти, що дає змогу істотно розширити масштаби освітнього простору та забезпечити можливість доступу все більшої частини населення до освітніх ресурсів певної країни та інших країн світової спільноти;

– перегляд і радикальна зміна змісту освіти на всіх його рівнях, що обумовлено стрімким розвитком процесу інформатизації суспільства. Ці зміни орієнтуються не тільки на все більшу загальноосвітню і професійну підготовку осіб, які навчаються у галузі інформатики, але також і на вироблення якісно нової моделі підготовки державних службовців до діяльності в умовах постіндустріального інформаційного суспільства, формування у них абсолютно нових, необхідних для цих умов, особистих якостей і навичок.

Навчання державних службовців із застосуванням дистанційних освітніх технологій передбачає інтеграцію традиційного уроку і кейсові технології дистанційного навчання, де контент (кейс) представлений у вигляді електронного посібника, призначеного для самостійного вивчення і формування основ комунікативної компетенції. Акцент за такого навчання ставиться на самостійній активній діяльності державного службовця [9].

Електронний посібник має модульну будову, низку специфічних рис і формується на засадах комунікативно-когнітивного підходу до навчання [10]. За сучасних умов реформування, інформатизації, варіативності та диференційованості освіти електронний посібник є важливим засобом методичного забезпечення навчального процесу, що охоплює цілі, зміст, дидактичні процеси та організаційні форми [11]. Методика використання дистанційних освітніх технологій у професійній підготовці державних службовців передбачає специфічні форми, методи, засоби та прийоми навчання і забезпечує готовність до оволодіння основами іншомовної комунікативної компетенції.

Сфери завдань публічного адміністрування курсів електронного навчання із застосуванням дистанційних інформаційних технологій у навчальному процесі державних службовців зазвичай окреслюють такими поняттями: «комунікативна компетенція», «дидактичний потенціал», «комунікативно-когнітивний підхід». Цей поділ орієнтується на історичну диференціацію сфери освітніх послуг. У контексті організаційних складових інтегрування курсів

електронного навчання із застосуванням дистанційних інформаційних технологій у навчальний процес державних службовців щодо структури завдань і заснованій на ній концепції адміністративно-правового регулювання передусім вирізняється інша класифікація типів, зокрема: інформаційне забезпечення навчання, інформаційна підтримка й освітнє публічне адміністрування за посередництвом третіх осіб.

Підсумовуючи вищевикладене, слід зауважити, що державне управління в українському суспільстві на шляху до інформаційного, заснованого на економіці знань, де ключову роль виконує інтелектуальний потенціал, висуває до професійної підготовки державних службовців в умовах адміністративної реформи в Україні нові вимоги: всебічність, доступність і своєчасність оновлення автентичного матеріалу (зміст навчання); широке охоплення аудиторії, незалежно від місця і часу звернення; використання сучасних інформаційних технологій; індивідуальний диференційований підхід до вибору зручних форм і методів навчання; створення комфортних умов для навчання; забезпечення гарантії якості освіти.

Створення єдиної системи електронного навчання не повинно перешкоджати самостійності освітніх установ і розвитку різноманітних форм електронного навчання, що забезпечують дотримання вимог державного освітнього стандарту. Проте, поряд із основними вимогами, що висуваються до установ електронної освіти, до установ дистанційної освіти у сфері професійної підготовки державних службовців в умовах адміністративної реформи в Україні доцільно законодавчо закріпити такі додаткові вимоги: всебічність, доступність і своєчасність оновлення автентичного матеріалу (зміст навчання); широке охоплення аудиторії, незалежно від місця і часу звернення; використання сучасних інформаційних технологій; індивідуальний диференційований підхід до вибору зручних форм і методів навчання; створення комфортних умов для навчання; забезпечення гарантії якості освіти.

Список використаної літератури:

1. Udaya Sri K. T. V. E-Learning: Technological Development in Teaching for school kids / Sri K. Udaya, Krishna Vamsi // International Journal of Computer Science and Information Technologies. 2014.

P. 6124–6126. URL: <http://www.ijcsit.com/docs/Volume%205/vol5issue05/ijcsit2014050527.pdf>

2. Changing Course. Ten Years of Tracking Online Education in the United States. Babson Survey Research Group. 2013. 42 p.

3. Хортон У. Электронное обучение: инструменты и технологии». У. Хортон, К. Хортон. СПб.: Кудиц-Образ, 2005. 640 с.

4. Меллинг М. Электронное обучение. Рекомендации руководителям библиотечных и информационных служб. М. Меллинг Supporting E-learning: A Guide for Library and Information Managers. М. Меллинг. М. : Омега-Л, 2006. 224 с.

5. Мауль А. В. Дидактическая целесообразность применения компьютерных учебников и обучающих систем. А. В. Мауль. Инновационные педагогические технологии : материалы междунар. науч. конф. (г. Казань, 14 октября 2014 г.). Казань : Бук, 2014. С. 300–302. URL: <http://www.moluch.ru/conf/ped/archive/143/6199/>

6. Інноваційні комп'ютерні технології у вищій школі : матеріали 6-ї наук.-практ. конференції (м. Львів, 18–20 листопада 2014 р.) відп. за випуск Л. Д. Озірковський. Львів : Вид-во Львівської політехніки, 2014. 196 с.

7. Використання інструментів міжнародної технічної допомоги Європейського Союзу як передумова ефективної модернізації державного управління в Україні. Т. О. Горецька. Ефективність державного управління. - 2012. Вип. 32. С. 346-353. URL: http://nbuv.gov.ua/UJRN/efdu_2012_32_45

8. Калінічева Г. І. Імплементация европейской системы обеспечения качества вищої освіти в Україні: досвід і перспективи. Г. І. Калінічева. Наук. вісник Чернівецького ун-ту : зб. наук. праць. 2009. № 2. С. 66–70.

9. The Standards and Guidelines for Quality Assurance in the European Higher Education Area ESG 28.09.2014. URL: <http://www.enqa.eu/index.php/home/esg/science>.

10. Blended learning. URL: <http://www.scoop.it/t/blended-learning-by-v-kukharenko>.

11. Annenkov I. P. Monitoring the quality of education in universities. – Available from (from title screen (in Ukrainian)). URL: <http://e-learning.onu.edu.ua/stati/pedagog-ka-visho-shkoli/an-nkova-p-mon-toring-jakost-osv-ti-u-vnz.html> Dividers.

Мельник Е.А.

кандидат філософських наук, доцент,
доцент кафедри правових наук та
філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського;

Конотопенко О.П.,

кандидат філософських наук, доцент,
доцент кафедри правових наук та
філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського;

Пилипенко Т.І.,

ст. викладач кафедри правових наук
та філософії Вінницького державно-
го педагогічного університету імені
Михайла Коцюбинського

ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНА КОМПЕТЕНТНІСТЬ КЕРІВНИКА В УМОВАХ ТРАНСФОРМАЦІЇ СИСТЕМИ ВИЩОЇ ОСВІТИ

Одним з важливих пріоритетів сучасної освіти в Україні є управління модернізацією національної освітньої системи, виважена й чітко спланована координація взаємодії суб'єктів освітньої політики, переосмислення функцій вищої освіти з екстраполяцією на майбутні перспективи, набуття нею особливого значення як рушійної сили позитивних змін у державі.

Реформування освітньої галузі ставить за мету створення привабливої та конкурентоспроможної національної системи вищої освіти України, яка інтегрується у Європейський простір вищої освіти, а також у Європейський дослідницький простір [1].

Так розвиток інформаційного суспільства, висувуючи нові вимоги до світової освітньої системи і до системи вищої освіти України зокрема, актуалізує підготовку та перепідготовку управлінців. Знання як ключовий показник якості освіти та кваліфікації пра-

цівника вже не є визначальним фактором професійної підготовки керівника. Сучасний конкурентоспроможний успішний керівник у сфері освітніх послуг зобов'язаний демонструвати стійкі навички використання інформаційно-комунікаційних технологій, критичного мислення, стратегічного планування, здатність гнучко реагувати на зміни потреб суспільства.

Прогнозування керівником кризових ситуацій, загострень соціальних суперечностей і проблем, тенденцій протидії і гальмування, вирішення їх, виходячи з принципів і закономірностей інформаційного суспільства потребує відповідних механізмів. Одним з таких механізмів соціальної еволюції, що забезпечує саморегулювання політичних, ідеологічних, інформаційних громадських підсистем є інформаційна культура.

Оскільки проблема формування і розвитку інформаційної культури керівника переходить на особистісний рівень, вона знаходить свій прояв у інформаційній поведінці, а також у формуванні інформаційного світогляду управлінця.

Інформаційна поведінка характеризується вміннями і навичками здійснення інформаційних операцій, оперування інформацією, здатність до саморегуляції і самоаналізу власного інформаційного поля і власної поведінки. Інформаційна культура дозволяє керівнику будувати комфортні та ефективні взаємини з навколишнім культурним середовищем, може слугувати інтегральним показником рівня розвитку суспільства і індивіда.

Процес формування інформаційної культури керівника-управлінця спонукає до створення необхідних компетентностей. Так звернення до статті 12 Закону України «Про освіту» розкриває поняття «інформаційно-комунікаційна компетентність» (далі – ІКК), що трактується не лише як цифрова грамотність, а й упевнене оперування, обмін і використання інформації в освітніх цілях.

Питанням компетентнісного підходу, формування педагогічної та професійної компетентності присвячено наукові розвідки таких зарубіжних та вітчизняних учених, як В. Байденко, Н. Бібік, О. Бондарчук, І. Зязюн, Л. Карамушка, Н. Клокар, І. Колеснікова, Н. Кузьміна, М. Лук'янова, А. Маркова, А. Москальова, О. Овчарук, Є. Рогов, О. Савченко, В. Сластьонін, В. Сериков, М. Скрипник,

М. Смутьсон, Т. Сорочан, М. Степко, Л. Хоружа. До питань медіа-технологій і медіаосвіти звертались такі дослідження Л. Баженової, Е. Бондаренко, Б. Гершунського, В. Грошева.

Огляд і узагальнення відповідних літературних джерел дає змогу зробити висновок, що науковці описують структуру компетентності фахівця-управлінця на основі кількох підходів: когнітивного, функціонального, особистісно-діяльнісного, що відображають зміни поглядів науковців на визначення та структуру компетентності. Наприклад, у 60-70-х роках ХХ століття компетентність розглядали як систему знань, професійну обізнаність керівника, а для опису її структури застосовували когнітивний підхід. Пізніше був запропонований компетентнісний підхід, який складали функціональний (опис структури на основі вмінь, навичок та функцій, які він має виконувати у своїй професійній діяльності) та особистісно-діяльнісний (особистість є суб'єктом діяльності та продуктом соціального розвитку). До складу останнього входять мотиваційно-ціннісний, когнітивно-діяльнісний, рефлексивний компоненти.

Так мотиваційно-ціннісний компонент стосується наявності у керівника мотивації (джерело активності й, одночасно, система спонукань будь-якої діяльності) та психологічної готовності до розвитку (саморозвитку) ІКК з огляду на її наявність (або відсутність) і необхідний рівень для виконання професійних обов'язків або життєдіяльності в інформаційному суспільстві.

Рефлексивний компонент, у свою чергу, «передбачає здатність до саморефлексії, саморегулювання, уміння здійснювати адекватну самооцінку розвитку ІКК. Для успішної рефлексії особистої ІКК керівник має розвивати в собі педагогічну самосвідомість, самооцінку, самоконтроль, набути професійну ідентичність» [2]. Адже рефлексія виконує синтезуючу роль і уможливорює розширення меж особистості. Саме тому керівник-лідер має розвивати складові емоційного інтелекту, серед яких: емоційна самосвідомість, точна самооцінка, упевненість у собі; емоційний самоконтроль, відкритість, уміння пристосуватись, цілеспрямованість, ініціативність, емпатія, або співпереживання; керування взаєминами, що в цілому буде сприяти змінам в організації.

Інтуїція – важлива якість для керівника, що полягає у застосуванні не лише технічних вмінь, а й життєвій мудрості до ухвалення

ділових рішень. Вона є природною для самосвідомого керівника. Дослухання до самовідчуттів допомагає знайти оптимальне вирішення ситуації і ухвалити найкраще рішення.

Серед висунутих ідей гуманітаризації, фундаменталізації, регіоналізації освіти як взаємодії суб'єктів освітнього процесу найбільш значущою є ідея, орієнтована на особистісний саморозвиток і навчання на цій основі рефлексивній діяльності. Вхідження рефлексії в науково-понятійний апарат досліджень обумовлено потребами розуміння ролі і статусу освіти, на який зверталася увага вчених (К. Абдульханова-Славська, Б. Братусь, Б. Вульф, О. Леонтьєв, В. Мухіна, О. Петровський та ін.).

Доцільно звернути увагу і на когнітивно-діяльнісний компонент, який стосується безпосереднього використання ІКК керівником у своїй професійній сфері, формування якого здійснюється одночасно у двох напрямках: з одного боку – формування користувацьких умінь у галузі ІКТ, а з іншого – формування вмінь використання інформаційно-комунікаційні технології (ІКТ) як ефективного засобу для підвищення якості освіти.

ІКК керівника під час використання ІКТ в освітньому процесі проявляється як операційна та методична компетентності. Операційна компетентність – сукупність знань і вмінь, а також досвіду, що дають змогу ефективно вирішувати проблеми, які виникають у процесі використання програмного й апаратного забезпечення. Слід звернути увагу на те, що керівник не має бути експертом, але мусить досягнути такого рівня володіння апаратним і програмним забезпеченням, щоб самостійно й оперативно, без спеціалізованої допомоги вирішувати будь-яку нагальну проблему під час використання ІКТ як і в освітньому процесі, так і в управлінській діяльності. Наприклад: знати, як користуватися найбільш розповсюдженими програмами доступу до глобальної мережі Інтернет та пошуковими системами, бути готовим до застосування апаратних і програмних засобів для проведення відеоконференцій (вебінарів) як у межах освітнього закладу, так і з іншими освітніми закладами.

Методична компетентність із використання ІКТ в освітньому процесі передбачає вміння застосовувати потенціал ІКТ для вдосконалення методики навчання своєї навчальної дисципліни. Вод-

ночас до переліку загальних ключових компетенцій, прийнятих Радою Європи у 1996 році, та якими повинні володіти молоді європейці [2], входять політичні й соціальні компетенції: здатність брати на себе відповідальність, підтримувати демократичні інститути тощо; міжкультурні компетенції – здатність прийняти інші культури, мови та релігії, виявляти повагу один до одного тощо. Тому, когнітивно-діяльнісну компоненту ІКК керівника доцільно доповнити такою складовою, як компетентність в етично-правових, соціальних і культурних питаннях, пов'язаних з інтеграцією ІКТ в освітню галузь. Наприклад, право на приватність передбачає нерозголошення керівником особистої інформації підлеглого [3].

Слід зазначити, що керівник також не має сліпо реалізовувати міністерські вимоги та освітянські рішення, миттєво впроваджувати у дію державно-нормативні документи, а творчо переосмислювати їх відповідно до ввіреного йому навчального закладу, вибудовувати управлінські рішення у процесі суб'єкт-суб'єктної взаємодії з колективом, через спільне критичне обговорення, поетапний аналіз та синтез кожної із запропонованих дій. Важливе значення при цьому відводиться розвитку педагогічного мислення як самого управлінця, так і кожного члена колективу, його здатності відображати педагогічну дійсність, педагогічний процес шляхом їх повноцінного пізнання і цілеспрямованого переосмислення. Також управлінець має критично ставитися і до нормативно-правових актів, постійно переглядати ієрархію цінностей та освітніх пріоритетів відповідно до вимог часу, рівня розвитку довіреного йому колективу й суспільства в цілому.

Водночас нове мислення не дозволяє управлінцеві використовувати готові, взяті з Інтернету шаблони для вирішення педагогічних завдань, при реалізації яких людина перебуває на репродуктивно-му рівні сприймання й відтворення інформації. Інформаційно-комунікативні технології мають виступати достовірним джерелом філософських та психолого-педагогічних ідей, що потребують переосмислення у конкретній освітній ситуації.

Водночас, суб'єкт-суб'єктна взаємодія покладає на управлінця моральну відповідальність за комфортність кожного члена колективу під час реалізації управлінських рішень, урахування їх погля-

дів на ту чи іншу вимогу. Тому при реалізації інформаційно-комунікативних технологій ми вважаємо за доцільне урахувати когнітивний стиль як основу педагогічного мислення кожного з членів колективу. На основі комплексного моніторингу індивідуально-психологічних особливостей сприймання та переосмислення інформації, її практичного застосування всіх членів колективу можна поділити на чотири групи: «активісти», «мислителі», «теоретики», «прагматики»:

«Активісти» – краще усвідомлюють суть управлінської проблеми та визначають шляхи її вирішення під час активної практичної діяльності, самостійних досліджень. Для них можна використовувати такі форми пізнання і переосмислення інформації для прийняття й реалізації управлінських рішень, як тренінгові заняття, «мозкові штурми», диспути, «круглі столи», «відкриті трибуни» тощо.

«Мислителі» – краще усвідомлюють суть проблеми, коли їм дається час на роздуми, спостереження, обдумування, схильні спостерігати за судженнями інших, послідовністю чужих думок, головне, щоб їм було досить часу для індивідуальної роботи та самоаналізу. Ефективними в роботі з ними є створення на основі запропонованої в мережі Інтернет інформації, власних проєктів реалізації управлінських рішень, власної моделі розв'язання освітньо-педагогічних завдань, обґрунтування її доцільності й ефективності в конкретних умовах; вибір із сукупності поглядів педагогічної спільноти на ту чи іншу тему тощо.

«Теоретики» – прагнуть пізнати, яким чином нова інформація вписується в уже відомі правила і концепції; схильні до аналізу і синтезу; мають логічне, теоретичне мислення, мислять абстрактними поняттями; люблять організованість і зрозумілість, роботу за планом чи графіком; уникають ситуацій, коли немає можливості задати запитання, проявити сумніви. Їх доцільно залучати до групи «експертів» для аналізу педагогічних теорій, методичних систем, технологій, розміщених у ресурсній базі мережі Інтернет.

«Прагматики» – схильні до рішення практичних завдань, надають перевагу знанням, що належать до реальних педагогічних ситуацій, мають практичне застосування, у пізнанні та переосмисленні

інформації керуються запитанням «Де я зможу це використати?», не люблять нічого ускладненого, пов'язаного з чистою теорією, орієнтацією на минуле чи майбутнє замість теперішнього. Вони із задоволенням користуються соціальними серверами, що дозволяють спілкуватися із такими ж як вони педагогами-практиками. У суб'єкт-суб'єктній взаємодії, спрямованій на прийняття та реалізацію того чи іншого управлінського рішення, педагоги-«прагматики» чітко знаходять практичну значущість, раціональну основу в чистій теорії.

Отже, для інтеграції у Європейський простір вищої освіти і створення конкурентоспроможної національної системи вищої освіти України нагальною необхідністю постає формування управлінської інформаційної культури, що реалізується в інформаційно-комунікаційних компетенціях керівника.

Література:

1. Концепція розвитку освіти України на період 2015–2025 років: проект. URL : https://docviewer.yandex.ua/view/62226167/?*=3D%3D&lang=uk.
2. Психолого-педагогічні особливості навчання керівних кадрів освіти заочно-дистанційною формою підвищення кваліфікації: акмеологічний підхід /Л. Л. Ляхощка // Вісник післядипломної освіти : зб. наук. пр. : у 2 ч. / Ун-тменедж. освіти НАПН України. – К.: АТОПОЛ, 2013. – Вип. 9 (22). – Ч. 1. –С. 129–140.
3. Брижко В.М., Пилипчук В.Г. Приватність, конфіденційність та безпека персональних даних / В.М.Брижко, В.Г. Пилипчук // Інформація і право. – Київ. – 2020. – № 1(32) – с. 33-46.

ЗАХИСТ ПРАВ, СВОБОД І БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ КАРАНТИНУ

Фурашев В.М.

кандидат технічних наук, старший
науковий співробітник, доцент

ІНФОРМАЦІЙНЕ ПРАВО ТА ПАНДЕМІЯ КОРОНОВІРУСУ COVID-19: ЗВ'ЯЗОК ТА НАСЛІДКИ

Згадаємо, що:

– головною метою інформаційного права є встановлення правовідносин в інформаційній сфері, тобто інформаційних правовідносин, загальних для всіх сфер забезпечення життєдіяльності суспільства та його розвитку;

– інформаційна безпека є невід'ємною складовою інформаційного права у частині загального поводження з інформацією та національної безпеки у частині спеціалізованого спрямованого поводження з інформацією;

– кібернетична безпека (кібербезпека) є складовою інформаційної безпеки як у частині загального поводження з інформацією, так і у частині спеціалізованого спрямованого поводження з інформацією, але із застосуванням кіберпростору. Кібербезпека є також невід'ємною складовою національної безпеки, але через інформаційну безпеку, як більш широкого за своєю сутністю.

Таким чином, інформаційне право займає вагоме місце у правовій системі, має своє власне «навантаження» і виконує визначену функціональну роль.

На жаль, більшість «класичних» юристів, включаючи досить багато вчених за науковою спеціальністю 12.00.07, поки ще не розуміють цього. Вони вважають, що правовідносини в інформаційній сфері достатньо повно відображаються адміністративним та господарським правом. Це недалекоглядна позиція та велика помил-

ка, яка з часом стане очевидною, але розуміння цього може прийти із запізненням.

Крім того, слід звернути увагу ще на один аспект. Правовідносини, в тому числі й інформаційні, та забезпечення їх дотримання є одним з головних атрибутів державності. Правовідносини мають як дозвільний характер, так і заборонний. Порухення встановлених правових норм уже класифікуються як правопорушення зі всіма наслідками. Правопорушення бувають свідомими або несвідомими, що виникають внаслідок необізнаності або різного законодавчого трактування одних і тих же дій. Особливо це стосується сучасних інформаційних правовідносин. Правовідносини заборонного або обмежувального характеру, в силу людської природи, не дуже сприймаються суспільством, як і будь-які примусові дії.

У той же час необхідно зазначити, що сукупність вже реалізованих досягнень науки і техніки майже у всіх сферах життєдіяльності суспільства вказує на необхідність зміни існуючої соціально-економічної світової моделі. Сучасна соціально-економічна модель, яка є породженням глобалізації фінансово-економічного та інформаційного простору, стає дедалі більшим стримуючим фактором науково-технічного прогресу та подальшого розвитку загальносвітового суспільства. Зважаючи на ці тенденції розвитку науково-технічного прогресу, нова соціально-економічна модель вимушена буде базуватися, у першу чергу, на тотальному контролі життєдіяльності кожної людини та формуванні «необхідного» світогляду. Такий світогляд буде суттєво, а може – кардинально, відрізнитися від теперішніх уявлень про основні права та свободи людини.

Виникає питання, яке відношення до викладеного має пандемії коронавірусу COVID-19? Відповідь дуже коротка – безпосереднє. Чому?

Коли уважно придивитися до протівірусних заходів у країнах світу та ще у сукупності з реальними та прогнозованими наслідками сучасного науково-технічного прогресу, а також тенденцій його подальшого розвитку, то складається відчуття, що пандемія, природна або штучна, виступає або використовується у якості одного із засобів цих змін.

Вже зараз можна стверджувати, що «допандемійний» та «післяпандемійний» світи будуть різними. У новій реальності будуть

інші бачення на акценти та механізми подальшого розвитку, формуватися відмінні від нинішніх міждержавні відносини, а також суспільні відносини на всіх рівнях.

Цілком природньо, сьогодні спостерігається суттєве зміщення акцентів у правовому регулюванні суспільних відносин та у структурі права.

Вже на даний час можна констатувати фактичну ліквідацію таких понять (юридичних інституцій), як «персональні дані», «приватне життя», «конфіденційна інформація» та ін. Під загрозою суттєвої трансформації знаходиться поняття «інтелектуальна власність».

У той же час змінюються акценти у бік посилення обмежувальних і регулятивних напрямів формування нових суспільних відносин під час використання інформаційного простору та встановлення нових правовідносин у частині поведінки з інформацією.

Підсумовуючі, можна сказати, що несприйняття, ігнорування або недостатня увага до інформаційного права як самостійної та однієї з визначальних галузей сучасного права – це шлях в нікуди.

Денисенко Н.В.

викладач кафедри філософії НТУУ
«Київський політехнічний інститут
імені Ігоря Сікорського»

ОБМЕЖЕННЯ ПРАВ ЛЮДИНИ ПІД ЧАС КАРАНТИНУ: ЧИ ІСНУЄ ЗАГРОЗА ДЕМОКРАТІЇ?

Сьогодні серед експертів точаться дискусії стосовно того, яким буде світ після пандемії коронавірусу. Ми можемо спостерігати наявність різноманітних сценаріїв. Але не дивлячись на їх відмінність, всі експерти констатують, що світ змінився. Зауважимо, що такі зміни спостерігаються з відповідною періодичністю. Остання найяскравіша зміна відбулася, коли у глобалізованому світі сталося «11 вересня». Тоді страхи тероризму дозволили обмежити права і свободи громадян. Треба відзначити, що таке обмеження сталося чи не вперше після боротьби за права людини на Заході кінця 60-х і точно – з 90-х років. Навіть, якщо згадати, відомий твір Фукуями «Кінець історії», що вийшов у 1992 році, і який було присвячено перемозі лібералізму. І тоді, в 90-ті здавалося, що права і свободи людини не будуть обмежені ніколи. Але як показує історія, це не так. Обмеження прав, які обґрунтовувалися особистою безпекою та захистом від тероризму, охопило світ з 2001 року. Тоді видавалося, що це буде мати тимчасовий характер. Але – з точки зору сьогодення – виявилося, що ні. Контроль держави над особистою свободою людини лише посилювався.

На жаль, теж саме ми спостерігаємо і зараз – коли держави, які раніше були зразком «західної моделі», почали переймати методи Китаю, – країни, де комуністичний тоталітаризм переріс в псевдокомуністичний інформаційний неототалітаризм, де держава контролює більшість сфер життя людини. Особливо це проявилось під час введення карантинних обмежень по всьому світі. І, як показує досвід, коли йдеться про тимчасові обмеження – вони можуть залишитися на невизначений термін. Останнє не може не викликати занепокоєння, що свободи і права громадян можуть не повернутися в «докарантинний» стан, а в посткарантинному світі

китайська модель тотального контролю може набути популярності. Вже сьогодні її демонструють як найдієвіший метод у протидії загрозам людства.

У зв'язку з пандемією коронавірусу в більшості країн світу було запроваджено велику кількість обмежень у повсякденному житті, що почало викликати занепокоєння серед широкої громадськості та правозахисників щодо порушення свобод і прав людини. З'явилися побоювання, що певні обмеження можуть залишитися в силі й після завершення пандемії. «COVID-19 – це тест для наших суспільств, і ми всі навчаємося та адаптуємося, реагуючи на вірус. Людська гідність і права людини повинні бути в центрі цих зусиль, а не другорядним питанням, про яке згадують запізно», – зазначає Мішель Багелет Верховний комісар ООН із прав людини. Дійсно, під час карантину ми спостерігали широкі обмеження прав і свобод людини. Але оскільки людина, її життя, здоров'я і безпека – це, відповідно до чинної Конституції України, найвища соціальна цінність, такі обмеження можуть бути цілком обґрунтованими. Вони, згідно з рекомендаціями ООН «Human rights at the time of COVID-19 – a Guidance Note», мають бути пропорційними, необхідними і недискримінаційними.

Коли ми говоримо про такі особливі режими у державі як карантин або, навіть, надзвичайний стан, ми маємо розуміти, що забезпечуються ці режими головним чином шляхом обмеження основних прав людини. Тому, в ці періоди як ніколи важлива оцінка дій держави з втручання у права людини: наскільки вони є обґрунтованими, необхідними, та чи дійсно вони переслідують саме мету захисту.

З яких джерел громадянин може дізнатись про свої права людини? Основні нормативно-правові акти, які містять такий перелік – Конституція України (Розділ II – Права, свободи та обов'язки людини і громадянина), Конвенція про захист прав людини і основоположних свобод, Міжнародний пакт про громадянські та політичні права. Важливо розуміти, що держава є гарантом прав людини. Разом з тим, вона також має право через свої державні органи і посадових осіб обмежувати практично всі права людини, але виключно на законних підставах. Потрібно пам'ятати, що є тільки два права, які ніколи не можна обмежувати: свобода від тортур і від рабства. Все інше може бути обмежене, якщо того вимагає ситуація.

11 березня Кабінет Міністрів України у постанові № 211 «Про запобігання поширенню на території України коронавірусу COVID-19» запровадив у нашій державі карантин. Карантин, згідно зі статтею 1 Закону України «Про захист населення від інфекційних хвороб», – це адміністративні та медико-санітарні заходи, що застосовуються для запобігання поширенню особливо небезпечних інфекційних хвороб. Зокрема, йшлося про примусову термометрію та подальшу обробку конфіденційної інформації про особу без її згоди, заборону відвідувати заклади освіти її здобувачам, проводити масові заходи, окрім тих, що забезпечують роботу органів державної влади та органів місцевого самоврядування. Карантин встановлюється на період, необхідний для ліквідації епідемії чи спалаху особливо небезпечної інфекційної хвороби. Впродовж цього часу можуть змінюватися режими роботи підприємств, установ, організацій, вноситися інші необхідні зміни щодо умов їх виробничої та іншої діяльності (ч. 4 ст. 29).

17 березня Верховна Рада прийняла закон (реєстраційний номер 3219) “Про внесення змін до деяких законодавчих актів України, спрямованих на запобігання виникнення і поширення коронавірусної хвороби (COVID-19)”, яким введено адміністративну відповідальність за порушення правил щодо карантину людей (відповідальність – штраф до 3400 грн. для громадян, та до 17000 грн. – для посадових осіб) та посилено кримінальну відповідальність за порушення санітарних правил і норм щодо запобігання інфекційним захворюванням та масовим отруєнням (відповідальність до 3 років позбавлення волі).

2 квітня до цієї Постанови Кабінетом Міністрів України внесено зміни (Постанова № 255), що ще більше обмежили особисті, політичні, економічні, соціальні і культурні права громадян.

Так, обмеження торкнулися права на повагу до приватного життя – зобов’язання носити документи, що посвідчують особу, її спеціальний статус, підтверджують громадянство.

Обмежуються права на свободу та особисту недоторканність – це примусове поміщення громадян в обсервацію; на свободу пересування – заборона для окремих груп населення перетинати кордон, для всіх – пересуватися групою у складі більш, ніж двоє осіб, відвідува-

ти парки, сквери, зони відпочинку, лісопаркові та прибережні зони, спортивні та дитячі майданчики, особам до 14 років – перебувати у громадських місцях без супроводу батьків. Йдеться також про скасування транспортного сполучення, зупинку роботи метрополітену.

Обмеження торкнулися свободи мирних зібрань та свободи віросповідання, адже проведення релігійних заходів заборонили; права на освіту, адже відвідувати навчальні заклади також заборонили; і на доступ до медичної допомоги, тому що проводити планові операції та заходи з госпіталізації також тимчасово заборонили.

Не можна проводити культурні, розважальні, спортивні, соціальні, релігійні, рекламні та інші масові заходи; заклади громадського харчування, торговельно-розважальні центри, інші розважальні, спортивні, культурні заклади зобов'язали зачинитися.

Таким чином, ми бачимо, що заходи, які застосовувалися, мають дуже великий вплив на можливість реалізації своїх прав громадянами. Тому дуже важливо, щоб держава та окремі посадовці не допускали при цьому зловживань, порушень та необґрунтованих втручань.

У Європі також 750 мільйонам мешканців довелося пережити суворе обмеження права на свободу пересування та інших прав і свобод. Згідно з міжнародним правом, заходи, які обмежують свободу пересування та інші права, повинні бути суворо необхідними, пропорційними, обмеженими в часі, здійснюватися для законних цілей (приміром, для охорони здоров'я населення) і застосовуватися без дискримінації. У багатьох країнах застосовувався режим суворого карантину і вживалися безпрецедентні заходи для боротьби з коронавірусом. Епідемія COVID – 19 стала серйозним викликом для правозахисників. Обмеження свободи пересування, заборона виходити на вулицю в деяких країнах – це те, з чим традиційно демократичні і вільні країни Західної Європи не стикалися з часів Другої світової війни. На тлі того, як у Європі запроваджувалися дедалі більші обмеження у щоденному житті, з'явилися побоювання, що певні заходи можуть залишитися і після завершення пандемії. Масштаби обмежень у різних країнах були неоднаковими. Так, життя громадян, приміром, у Франції та Італії було майже паралізовано, а за порушення стягувалися чималі штрафи. В Італії мінімальний штраф було встановлено в розмірі 400 євро. Ті, хто

мав підтверджений діагноз COVID-19 за порушення карантину могли опинитися у в'язниці. Деякі заходи, які вживалися в Європі, були менш помітні, але саме вони викликають занепокоєння щодо дотримання прав людини. Приміром, оператори мобільного зв'язку в Італії, Німеччині та Австрії ділилися даними користувачів з органами системи охорони здоров'я, допомагаючи контролювати, чи дотримуються люди заборони залишати оселю та вимоги уникати зайвих контактів. Дані були анонімними. Проте, витік даних на веб-сайті Міністерства охорони здоров'я Австрії вже викликав занепокоєння щодо захисту особистих даних. Кожна з європейських країн заявляла про відповідні терміни щодо безпрецедентних обмежень. Але одна з європейських країн обрала дуже суперечливий шлях – це Угорщина, парламент якої схвалив проект про безстрокове продовження надзвичайного стану, надаючи прем'єр міністру широкі повноваження. Законопроект також передбачає ув'язнення як покарання для тих, хто поширює фейкові повідомлення про коронавірус чи заходи проти нього. Брюссель застеріг Угорщину щодо порушення верховенства права. Експерти стверджують, що власне встановлення терміну дії тих чи інших заходів є визначальним, коли йдеться про законність нових обмежень у Європі щодо свобод і прав людини. Важливо пам'ятати, що такі заходи згідно норм міжнародного права у галузі прав людини лише тоді є законними, якщо вони вважаються необхідними, виправданими та обмеженими в часі. Також необхідними є належний контроль, демократична дискусія та моніторинг усіх цих заходів.

Деякі країни ЄС уже мають досвід, коли надзвичайні заходи можуть тривати довше, ніж передбачалося. Візьмімо, приміром, Францію після терактів у Парижі 2015 року, коли уряд оголосив надзвичайний стан. Неурядові організації критикували, що виняткові повноваження перетворили на закон. Низка європейських країн, серед яких Латвія, Грузія, Естонія, Вірменія та Румунія вже оголосили про намір відійти від Європейської конвенції про права людини з огляду на пандемію коронавірусу. Конвенцією про захист прав людини і основоположних свобод допускається обмеження прав громадян, але лише у випадках, що передбачені законом і є необхідними в демократичному суспільстві для захисту здоров'я

людей. З позиції міжнародного права, певні обмеження прав людини також дозволяються лише в умовах надзвичайного стану. Наприклад, відповідно до Європейської конвенції про захист прав людини, під час війни або іншої суспільної небезпеки, яка загрожує життю нації, будь-яка із договірних сторін може вживати заходів, що відступають від її зобов'язань за цією Конвенцією, виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов'язанням згідно з міжнародним правом. Більше того, в ст. 12 Міжнародного пакту про економічні, соціальні та культурні права передбачається обов'язок держав вживати заходів для запобігання і лікування епідемічних, ендемічних, професійних та інших хвороб і боротьби з ними. Але ніде в міжнародних документах не передбачено, що ці заходи можуть супроводжуватись порушенням прав людини. Проте, правозахисники закликають бути обережними. Так, одна зі спецдоповідачів ООН написала у своєму мікроблозі: «Ми можемо пережити кризу в охороні здоров'я, але якщо ми не повернемося до наших демократичних цінностей – ми програли цю війну».

Президент Парламентської асамблеї Ради Європи Рік Дамс започаткував платформу у соціальних мережах #RACEvoices з метою підтримки прав людини в умовах режиму карантину, уведеного у багатьох європейських країнах через пандемію коронавірусу. «Коронавірус може віддалити нас, але не може примусити нас мовчати», – заявив президент ПАРЄ. Він закликав колег і громадян приєднуватися до платформи #RACEvoices заради захисту Європейської конвенції з прав людини, основоположних свобод, верховенства права і демократії.

Таким чином, щоб обмежити якісь права, держава повинна виконати ряд умов: мати чітку мету для обмеження, а заходи вводити необхідні і пропорційні. Якщо в Індії б'ють людей, що порушують карантин – це точно не пропорційні заходи. Що точно не заборонено в таких непростих умовах, то це поширення правдивої інформації про захворювання або про порушення громадянських прав. Отже, задля збереження життя й здоров'я людей, карантинні заходи мають право на існування, але за умови їх виправданості, адекватності та з метою суспільної необхідності. Важливо дотримуватися балансу

між правом однієї людини та правом всієї нації на здорове існування та безпечне середовище. І посадові особи держави повинні обґрунтовано приймати якісні нормативно-правові акти для розв'язання будь-якої проблеми, в тому числі й протидії пандемії коронавірусу.

У ситуації, що склалась, наступ на права людини є тестуванням суспільства на терпимість. Сьогодні в Україні широко точиться дискусія про те чи не надто сильним є «прикручування гайок» під прикриттям боротьби із коронавірусом. «Зупиняти машини і проводити обшуки - це буде ще ОК, чи вже занадто? А закривати некритичні підприємства чи торгові точки, навіть якщо там не планувалось скупчення людей, без жодної компенсації - це прийнятно чи не зовсім?» Уже сам факт обговорення таких питань свідчить про поступове підвищення межі терпимості суспільства до жорстких заходів і порушення прав людини. У суспільстві починає припускатися можливість щодо порушення прав людини і започатковується градація щодо прав, які ми дозволимо порушувати без законних на це підстав, а які - (поки що) не дозволимо. Нам пропонують «світовий досвід, який себе добре показав», ми чуємо про «ефективні методи в диктаторському Китаї» та інші тези, які заколисують нашу пильність, аби ми відчули себе «в одному човні» з усім світом і не запідозрили жодних девіацій у вітчизняному досвіді вирішення проблеми боротьби з коронавірусом. І на останок, і це найбільший ризик – ми можемо знайти себе в ситуації, коли порушення основоположних свобод і прав людини стане частиною повсякденного життя уже після завершення пандемії коронавірусу. Тому непорушність прав людини повинно бути аксіомою. І якщо зараз людство не стане на захист таких прав, у подальшому це буде ще складніше робити. І завжди варто пам'ятати – не має значення привід, під яким обмежуються певні права, якщо він незаконний. Навіть якщо такий привід звучить дуже глобально – «запобігти пандемії і врятувати людство». Саме тому активне громадянське суспільство, медіа, юридична спільнота, відповідальні політики повинні не стояти осторонь порушення фундаментальних основ демократії – основоположних свобод і прав людини, аби потім не розділяти відповідальність за встановлення в країні чергового модифікованого авторитарного чи навіть тоталітарного режиму.

Щириця Т.В.

кандидат філософських наук, доцент

МОРАЛЬНО-ЕТИЧНІ АСПЕКТИ ЗАХИСТУ ПРАВ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ ЗА УМОВ КАРАНТИНУ

Дослідження теми захисту прав людини має міждисциплінарний характер, тож слухними є такі розвідки: теоретико-методологічні, семантично-ідеологічні, соціально-психологічні, культурно-ментальні, морально-правничі, повсякденно-практичні тощо. Всі вони використовують специфічний науковий інструментарій, масштаби й форми опису, критерії істинності та формально-логічні запобіжники щодо хибних суджень, ціннісно-нормативні виміри і мету. Формування прав людини та їхній захист здійснюються на двох рівнях – державному й громадському. Відомим є факт того, що текст конституції П.Орлика мав майже бездоганний характер, проте імплементація норм основного закону не мала історично-культурного підґрунтя. Це не принижує правничий розум П.Орлика, радше свідчить про його інтелектуальний внесок в історичний ціннісно-світоглядний поступ українців від бездержавності до суверенності. І в такому поступі текст має велике значення.

Нова соціально-політична і безпекова ситуація в світі пов'язана із пандемією коронавірусу. Не будемо тут обговорювати причину його походження – природну чи штучну, рукотворну (в соціальних мережах і на різних платформах, зокрема й наукових, поряд з прагненням науковців до істини, часто-густо оприлюднюються різні фейки), скажімо тільки, що в його функціонуванні багато невизначеного, непізнаного, проте вкрай загрозливого щодо людини. З одного боку, епідеміологи наполягають на створенні колективного імунітету, тож багато людей мають перехворіти, з іншого боку, найпершим завданням є відтермінування функціонування COVID-19 аби уникнути великої чисельності хворих водночас. Саме для цього поширюються правила карантину.

В класичних політичних теоріях держава має монополію на використання примусових заходів задля досягнення певних цілей. Описуючи державу Левіафан (книга була видана в Лондоні у 1651 р.)

її автор Т.Гобс в своїй теорії суспільного договору наполягав на необхідності застосовувати примус задля виходу з природного стану «війна кожного проти кожного», «війна всіх проти всіх», «*homohominilupus*». Подолати природний стан й перейти до стану суспільства можна тільки через впровадження в тіло держави понять:природне право, природний закон, свобода й необхідність. Такі зміни в поступі людства утворюють між володарем і підданими суспільний договір, порушувати який неможна.

З тих часів змінюються й теорії, й практики державотворення. Окремі суспільства шукають зрозумілих для себе форм організації й самоорганізації, які засадничені базовими правами людей й методами їхнього гарантування й захисту. Відомий в Україні соціальний філософ М. Мінаков вважає, що в нас утворилася така держава, яка має два складники, а саме: складник держави як владної корпорації й складник держави як ресурсу для владарювання, тобто держава як здобич. Ці складники взаємо пов'язані, взаємо контрольовані і забезпечені відповідними правами й обов'язками. Така характеристика держави не відповідає сучасним вимогам загальнолюдських цінностей, нормам свободи, справедливості, солідарності, гуманності.

Хижацьке ставлення українського істеблішменту до природних і культурних багатств, їхня егоїстична нещадна експлуатація, стереотипи тимчасовості й необхідності скористатися ситуацією задля індивідуального прибутку, відсутність прагнення до всезагального блага, нехтування загальнолюдськими цінностями унаочнили кризу управління під час пандемії. Держава, яка захищає права окремих кланів, корпорацій, соціальних груп, виявилася неспроможною приборкати серйозну небезпеку коронавірусу. В її ресурсі є тільки заборона і захист прав тих, хто таку заборону здійснює. При цьому без гарантії й захисту прав залишилися люди тих професій, які стикаються із вірусом безпосередньо, передусім медичні працівники. Громадський загаль віднайшов способи захисту без участі держави, зокрема, українці пошили собі маски, раціонально обмежили соціальний простір, поглибили віртуальне спілкування, погодилися на матеріальні збитки, розгорнули просвітницьку діяльність в соцмережах тощо. Всі ці дії спрямовані на виправдан-

ня кризової ситуації та сприйняти необхідних обмежень не як порушення прав, а як їхній специфічний захист.

Зараз активно дискутується тема політичного устрою держави, яка ефективніше організувала карантинні заходи. Які структури перемогли: авторитарні чи ліберальні? Примус чи свобода? У який спосіб держава гарантувала громадянину захист права на життя? І яке життя? Я завжди згадую думку Сократа про те, що людина поціновує не життя як таке, а життя хороше, гідне. Зрештою, всі ми опинилися вдома на 2-3 місяці і як використали таку ситуацію? В Китаї після карантину зросла кількість розлучень, отже люди не змогли порозумітись на близькій відстані. А в Україні? Чи захистила держава та її інституції від стресів, депресій, зайвої ваги, непорозумінь? Ми можемо казати, що усталена правова система захисту не стала адекватною у ситуації форс-мажору. Тоді нам треба дискутувати з приводу оновлених прав людини. Бо ситуація обмеження соціального простору, на жаль, може повторитись.

Де кілька думок з приводу модернізації правничої сфери і правової свідомості через нестандартні соціальні умови пандемії. Формування та формулювання прав людини та їхній захист має відбуватись в аксіосфері загальнолюдських цінностей, імплементації в соціальні інституції й практики повсякденності базових прав, наголосі на персональній свободі, отже відповідальності. Формою утворення чи оновлення політико-правової сфери має стати найширші дискурси, в яких, на думку представників комунікативної теорії суспільства (Ю.Габермас, К.-О.Апель, Д.Бюлер, А.Єрмоленко), єдиним примусом є примус найвагомішого аргументу. Оскільки в інформаційне поле часто-густо потрапляють вигадані пропагандистські історії, які виглядають як правдиві, важко знайти підстави для їхнього логічного аналізу й висновку. Споживачі інформації звертають увагу не тільки на зміст, а й на джерела, ранжуючи їх через рейтинг або особистісну повагу й слушність. Переконались в правильності й чесності інформації дозволяє спілкування, зокрема й в формі нашої науково-практичної конференції, де інтелектуалами з різних наукових спеціальностей обговорюється складна тема захисту прав, свобод і безпеки людини в інформаційній сфері.

Проць І. М.

кандидат юридичних наук,
доцент кафедри адміністративно-
правових дисциплін Львівського
державного університету внутріш-
ніх справ

Ямкова Т.І.

здобувач вищої освіти
юридичного факультету Львівського
державного університету внутріш-
ніх справ

ЗАХИСТ ІНФОРМАЦІЙНИХ ПРАВ ПІД ЧАС КАРАНТИНУ

Карантинні обмеження суттєво обмежили права усіх людей. Деякий час ми не могли навіть вийти на прогулянку до парку, через загрозу інфікування. Але крім прав на звичайні буденні дії обмежили також і інформаційні права громадян, адже перебуваючи у самоізоляції дуже важко відділити правду від брехні.

Звісно, під час пандемії наше основне право це знати відомості про поширення хвороби, кількість її жертв та засоби запобігання захворювання. Якщо прочитати закони, що стосуються запобігання пандемії, то можна сказати, що права та свободи громадян щодо доступу до публічної інформації не обмежуються. Відповідно до статті 1 Закону України «Про доступ до публічної інформації», публічна інформація - це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні суб'єктів владних повноважень, інших розпорядників публічної інформації, визначених цим Законом (1). Майже все, що є реально у влади, органів місцевого самоврядування «в руках» (задокументовано) стосовно епідемії, розвитку подій, заходів, є публічною інформацією з відкритим порядком доступу. Це і кількість апаратів штучного дихання, і кількість тих чи інших препаратів наявних та необхідних, і кількість бюджетних коштів

будь-якого рівня, які витрачено і заплановано витратити і на що саме, і хто є постачальником, і плани реагування, і ті чи інші параметри щодо стану системи охорони здоров'я на будь-якому рівні, і кількість хворих, і кількість підозр на захворювання, і інформація про ціни на препарати, маски і т.д. Слід зазначити, що високий і майже незаперечний статус суспільної значущості теми надає право вимагати інформацію, яка будь-яким чином стосується епідемії, і у приватних юридичних осіб. Наприклад, відомості про формування і витрачання коштів (на що, кому, скільки, коли) з фонду, який має з'явитись після зустрічі президента з великим бізнесом – апріорі не можуть бути закритими в доступі. Навіть якщо оперувати ними буде якась благодійна або приватна організація.

Які обов'язки є у органів влади під час епідемій щодо публічної інформації? Стосовно інформаційної складової спеціальне законодавство у сфері протидії інфекційним захворюванням та епідеміям містить такі норми та гарантії:

- Закон України «Про забезпечення санітарного та епідемічного благополуччя населення» (статті 4, 6):

- Громадяни мають право на участь у розробці, обговоренні та громадській експертизі проектів програм і планів забезпечення санітарного та епідемічного благополуччя населення, внесення пропозицій з цих питань до відповідних органів;

- Громадяни мають право на достовірну і своєчасну інформацію про стан свого здоров'я, здоров'я населення, а також про наявні та можливі фактори ризику для здоров'я та їх ступінь;

- Підприємства, установи і організації мають право на одержання від органів виконавчої влади, місцевого самоврядування, а також відповідних органів і закладів охорони здоров'я інформації про стан здоров'я населення, санітарну та епідемічну ситуацію, нормативно-правові акти з питань забезпечення санітарного та епідемічного благополуччя населення та санітарні норми;

- Закон України «Про захист населення від інфекційних хвороб» (стаття 17):

- Громадяни та їх об'єднання мають право на отримання достовірної інформації щодо епідемічної ситуації в Україні.

– Органи виконавчої влади та органи місцевого самоврядування, органи державної санітарно-епідеміологічної служби та заклади охорони здоров'я зобов'язані періодично повідомляти через засоби масової інформації про епідемічну ситуацію та здійснювані протиепідемічні заходи.

– За відмову у наданні інформації, умисне перекручення або приховування об'єктивних даних про захворювання населення на інфекційні хвороби посадові особи органів, та закладів, зазначених у частині другій цієї статті, несуть відповідальність згідно із законом.

– Громадяни та їх об'єднання мають право брати участь в обговоренні питань щодо розміщення та будівництва об'єктів, що можуть негативно впливати на епідемічну ситуацію, проектів державних цільових, регіональних і місцевих програм з питань захисту населення від інфекційних хвороб і вносити пропозиції з цих питань до відповідних органів виконавчої влади та органів місцевого самоврядування, установ і організацій (2).

Закон “Про доступ до публічної інформації” визначає права громадян і обов'язки розпорядників публічної інформації (тобто тієї інформації, яка є в розпорядженні центральних органів влади, місцевих рад, виконкомів, комунальних підприємств, установ та організацій).

Люди можуть запитувати публічну інформацію (усно, письмово, електронною поштою). Відповіді мають бути надані протягом:

– 48 годин, якщо йдеться про захист життя чи свободи особи, стан довкілля, якість харчових продуктів і предметів побуту, аварії, катастрофи, небезпечні природні явища та інші надзвичайні події, що сталися або можуть статись і загрожують безпеці громадян;

– п'яти робочих днів у всіх інших випадках;

– відтерміновані на 20 робочих днів, якщо запит стосується надання великого обсягу інформації або потребує пошуку інформації серед значної кількості даних.

Розпорядники мають надавати повну відповідь на запит або обґрунтовано відмовити. Неповна відповідь, часткова, не по суті, відсутність відповіді – все це є порушенням закону і призводить до адміністративної відповідальності (3).

Проте з початком карантину деякі із депутатів хотіли внести поправки в законодавство щодо того, щоб із початком оголошення карантину зупинити перебіг строків розгляду на публічнізапити. Така пропозиція викликала обурення з боку захисників інформаційних прав, так як це звужує права особи на доступ до публічної інформації. Крім того таке положення порушує конституційні засади та положення Конвенції про захист прав людини і основоположних свобод.

Легко обмінюватися та отримувати дані про стан поширення коронавірусу можна на Єдиному порталі відкритих даних. Також отримати подібного роду інформацію можна на Європейському порталі відкритих даних.

Також, відповідно до підпункту 1 пункту 2 розділу II “Прикінцеві та перехідні положення” Закону України від 13 квітня 2020 р. № 555-IX “Про внесення змін до Закону України “Про захист населення від інфекційних хвороб” щодо запобігання поширенню коронавірусної хвороби (COVID-19)” дозволяється здійснювати обробку (в тому числі обмін інформацією в порядку, визначеному цією постановою) персональних даних осіб, визначених цією постановою як таких, що підлягають самоізоляції або обсервації (ізоляції):

медичним працівникам закладів охорони здоров’я - щодо внесення до зазначеної в абзаці першому цього пункту системи інформації в порядку, передбаченому цією постановою;

державній установі “Центр громадського здоров’я Міністерства охорони здоров’я України”, державним установам епідеміологічного профілю Міністерства охорони здоров’я, Міністерству цифрової трансформації – щодо прізвища, імені, по батькові особи, дати народження, визначеного особою місця самоізоляції, місця реєстрації, місця проживання особи, інформації про засоби зв’язку (номер телефону), місця роботи, навчання, коротких відомостей про стан здоров’я;

органам з питань соціального захисту населення - щодо прізвища, імені, по батькові особи, статі, дати народження, визначеного особою місця самоізоляції, місця реєстрації, місця проживання особи, інформації про засоби зв’язку (номер телефону);

Національній поліції, Національній гвардії – щодо прізвища, імені, по батькові особи, дати народження, визначеного особою місця самоізоляції, місця реєстрації, місця проживання особи, інформації про засоби зв'язку (номер телефону) з метою здійснення поточного контролю за дотриманням режиму самоізоляції та щодо осіб, які порушили правила щодо карантину, санітарно-гігієнічні, санітарно-протиепідемічні правила і норми, визначені цією постановою. Порядок інформаційної взаємодії Єдиного державного веб-порталу електронних послуг, інформаційних систем Міністерства внутрішніх справ та Національної поліції, інформаційних систем Міністерства охорони здоров'я, державної установи "Центр громадського здоров'я Міністерства охорони здоров'я України", Служби безпеки встановлюється Міністерством цифрової трансформації та держателем відповідної інформаційної системи в об'язі, необхідному для виконання цієї постанови (4).

Також, не варто забувати, що важливий внесок у забезпеченні наших інформаційних прав відіграють ЗМІ, адже саме журналісти добувають для нас те, що може приховуватися. Зокрема, частина 1 статті 25 Закону України «Про інформацію» гарантує журналістам право під час виконання професійних обов'язків здійснювати письмові, аудіо- та відеозаписи із застосуванням необхідних технічних засобів, за винятком випадків, передбачених законом. Це право також гарантовано журналістам пунктом 3 частини 2 статті 26 Закону України «Про друковані засоби масової інформації (пресу) в Україні», статтею 21 Закону України «Про інформаційні агентства». Отже, як видно з наведеного, журналісти мають право під час збору інформації використовувати необхідну техніку, в тому числі фотоапарати та відеокамери. Винятки із цього правила можуть бути передбачені лише законами, тобто актами, прийнятими Верховною Радою України. Жодні інструкції, накази чи інші підзаконні акти не можуть заборонити журналісту проводити зйомку.

12 березня 2020 року постановою Кабінету Міністрів України від 11 березня 2020 р. № 211 "Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2" на всій території України введено карантин з 12 березня 2020 року і визначено низку заходів протидії

поширенню цієї небезпечної хвороби. Перелік заходів запобігання пандемії постійно поповнюється й іншими рішеннями Уряду та місцевих рад. Оскільки дотримання цих правил впливає на можливість поширення хвороби, а значить і на кожного з нас, природно, що журналісти звертають увагу на зазначену тему і досліджують питання про те, хто, де і як виконує протиепідемічні заходи. І, що б не бути голослівними, фіксують це на відео (5). Але, при здійсненні своїх професійних обов'язків, журналісти повинні дотримуватися протиепідеміологічних правил, тобто, носити маски, рукавиці, дотримуватися соціальної дистанції.

Отже, інформаційні права під час карантину всіляко намагаються порушити, вносячи відповідні законопроекти. Але, українське законодавство, зокрема Конституція України, в першу чергу захищає права та свободи громадян від таких зазіхань. Основним правилом при таких умовах є фільтрування різного роду інформації та сприйняття лише тої, яка походить з пререверених джерел.

Список використаної літератури

1. Про доступ до публічної інформації: Закон України від 13 січня 2011 року № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17>
2. Доступ до інформації під час карантину – гарантії чи обмеження? URL: <https://dostup.pravda.com.ua/news/publications/dostup-do-informatsii-pid-chas-karantynu-harantii-chy-obmezhennia>
3. Чи приховують правду про коронавірус: шість тез щодо права на інформацію під час пандемії. URL: <https://zmina.info/articles/chy-pryhovuyut-pravdu-pro-koronavirus-6-tez-pro-pravo-na-informacziyu-pid-chas-pandemiyi/>
4. Постанова Кабінету Міністрів України від від 11 березня 2020 р. № 211 «Про запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2». URL: <https://zakon.rada.gov.ua/laws/show/211-2020-%D0%BF>
5. Консультація щодо права журналістів збирати інформацію та проводити відеозйомку в публічних місцях. URL: <https://www.ppl.org.ua/konsultaciya-shhodo-prava-zhurnalistiv-zbirati-informaciyu-ta-provoditi-videozjomku-v-publichnix-miscyah.html>

Лапшин С.А.

кандидат історичних наук,
доцент кафедри правових наук та
філософії Вінницького державного
педагогічного університету
ім. М. Коцюбинського

Гриб В.І.

кандидат філософських наук,
доцент кафедри правових наук та
філософії Вінницького державного
педагогічного університету
ім. М. Коцюбинського

ОСОБЛИВОСТІ ПОДАННЯ ДОКУМЕНТІВ ДЛЯ ЗДОБУТТЯ СТУПЕНЮ ВИЩОЇ ОСВІТИ МАГІСТРА В УМОВАХ КАРАНТИНУ (НА ПРИКЛАДІ РЕЄСТРАЦІЇ НА ЄВІ)

Пандемія коронавірусу вплинула на усі сфери життєдіяльності людини в усьому світі. Механізмом боротьби із нею стало запровадження жорстких карантинних заходів, спрямованих на обмеження соціальних контактів між людьми, їх пересування між населеними пунктами та ін. Водночас, переважна більшість процедур отримання адміністративних послуг, реалізація права на освіту (в тому числі і вступна кампанія) передбачала особисту присутність особи для подання необхідних документів. Нові суспільні реалії вимагають внесення змін у публічне адміністрування отримання відповідності послуг (в т.ч. здійснення освітньої діяльності), їх цифровізацію. Причому їх прийняття та реалізація вимагають оперативності у зв'язку із обмеженим періодом проведення вступної кампанії.

Вступна кампанії до закладів вищої освіти (далі – ЗВО) відбувається на основі нормативно-правової бази, яка складається із: Закону України «Про вищу освіту», Умов прийому (затверджуються щорічно), Правил прийому (затверджуються щорічно вченою радою ЗВО, формується на основі Умов прийому), інструкцій,

роз'яснень Міністерства освіти і науки України, Департаментів освіти обласних державних адміністрацій.

Вважаємо за необхідне подати визначення термінам вступник та єдиний вступний іспит, які є ключовими у нашій статті. Відповідно до Умов прийому до ЗВО, вступник це особа, яка подала заяву(и) про допуск до участі в конкурсному відборі на одну (декілька) конкурсних пропозицій; єдиний вступний іспит (далі - ЄВІ) - форма вступного випробування з іноземної (англійської, або німецької, або французької, або іспанської) мови для вступу на навчання для здобуття ступеня магістра на основі здобутого ступеня вищої освіти бакалавра, магістра (освітньо-кваліфікаційного рівня спеціаліста), яка передбачає використання організаційно-технологічних процесів здійснення зовнішнього незалежного оцінювання [1].

Набуття статусу вступника передбачає подання заяви (заяв) до ЗВО для участі у конкурсному відборі. Відповідно до Правил прийому до Вінницького державного педагогічного університету ім. М. Коцюбинського (далі - ВДПУ) вступники для здобуття ступеня магістра (крім спеціальностей галузей знань 01 «Освіта/Педагогіка» та спеціальності 025 «Музичне мистецтво») на основі здобутого ступеня вищої освіти або освітньо-кваліфікаційного рівня спеціаліста подають заяви:

1) тільки в електронній формі, крім визначених у цьому пункті випадків;

2) тільки у паперовій формі: для реалізації права на вступ за результатами вступних іспитів з конкурсних предметів у закладі вищої освіти та/або квотою для іноземців відповідно до цих Умов; для реалізації права на повторне безоплатне здобуття освіти за бюджетні кошти відповідно до цих Умов; для реалізації права на першочергове зарахування відповідно до цих Умов; за наявності розбіжностей у даних вступника в ЄДЕБО (прізвище, ім'я, по батькові, дата народження, стать, громадянство тощо) і у відповідному документі про здобуття ступеня (освітньо-кваліфікаційного рівня) вищої освіти, на базі якого відбувається вступ; у разі подання іноземного документа про освіту; у разі подання заяви іноземцями та особами без громадянства, які постійно проживають в Україні; у разі подання документа про здобуття ступеня (освітньо-кваліфі-

каційного рівня) вищої освіти, на базі якого відбувається вступ, інформація про який відсутня в ЄДЕБО; у разі подання заяви після завершення строків роботи електронних кабінетів; у разі неможливості зареєструвати електронний кабінет або подати заяву в електронній формі з інших причин, що підтверджено довідкою приймальної комісії закладу вищої освіти.

ЗВО можуть передбачити на вебсайті електронну реєстрацію на участь у вступному іспиті, творчому конкурсі за умови подання вступником сканованих копій (фотокопій) документів [2].

У зв'язку з запровадженням карантину Міністерство освіти і науки України надіслало ЗВО лист, в якому поінформувало про зміну порядку та термінів реєстрації вступників для складання ЄВІ з іноземної мови.

Докладніше проаналізуємо особливості та механізм подачі заяв для реєстрації на ЄВІ. Зокрема, реєстрація розпочинається з 9:00 12 травня та закінчується о 18:00 05 червня 2020 р. Реєстрації на ЄВІ вступників на навчання для здобуття ступеня магістра на основі ступеня вищої освіти (освітньо-кваліфікаційного рівня), здобутого за іншою спеціальністю (напрямом підготовки), передувало складання додаткових фахових вступних випробувань. Водночас, з 16 січня 2020 року набрав чинності Закон України «Про внесення змін до деяких законів України щодо вдосконалення освітньої діяльності у сфері вищої освіти», яким внесено зміни до Закону України «Про вищу освіту», зокрема, в частині скасування обов'язкового складання додаткових фахових вступних випробувань для вступників, які вступають на навчання для здобуття ступеня магістра на основі ступеня вищої освіти (освітньо-кваліфікаційного рівня), здобутого за іншою спеціальністю (напрямом підготовки). Таким чином необхідність проведення додаткових фахових вступних випробувань визначається Правилами прийому закладу вищої освіти.

ЗВО було запропоновано до 07 травня 2020 р. визначитись щодо необхідності проведення додаткових фахових вступних випробувань (далі – ДФВВ) та опублікувати відповідну інформацію на офіційних сайтах. Рекомендація скасування ДФВВ також викликана необхідністю обмеження пересування людей між населеними пунктами.

Враховуючи епідеміологічну ситуацію, що склалася в Україні, з метою запобігання поширенню коронавірусної хвороби (COVID - 19) Міністерство освіти і науки України рекомендувало ЗВО наступний алгоритм дій для реєстрації вступників для складання ЄВІ:

До початку періоду (не пізніше ніж за три дні), відведеного для реєстрації осіб, які виявили бажання брати участь у конкурсному відборі на навчання для здобуття ступеня магістра за спеціальностями, визначеними пунктами 5, 6 розділу V Умов прийому до ЗВО України, затверджених наказом Міністерства освіти і науки України № 1285 від 11 жовтня 2019 року, зареєстрованим у Міністерстві юстиції України 02 грудня 2019 року за № 1192/34163 (далі – реєстрація), заклади вищої освіти розміщують на своїх офіційних веб-сайтах електронну адресу Приймальної комісії, зазначену в Реєстрі суб'єктів освітньої діяльності ЄДЕБО, для отримання копій документів осіб, які бажають взяти участь у вступних випробуваннях (далі – вступники), а також номери телефонів, за якими вступник може отримати консультацію. Водночас, ЗВО можуть додатково використовувати інші канали обміну інформацією (власні системи, jotforms тощо) за умови розміщення відповідної інформації на сайті закладу і забезпечення можливості використання офіційної електронної адреси Приймальної комісії [3].

Після отримання зазначених документів відповідальна особа Приймальної комісії здійснює реєстрацію вступника, оформлює екзаменаційний листок та особову справу вступника.

Таким чином, в умовах карантину, обмеження соціальної взаємодії між людьми реєстрація на ЄВІ для вступу до ЗВО відбувається виключно за допомогою цифрових технологій без особистої присутності вступника. Також, ЗВО надано автономне право визначити доцільність проведення ДВФВ, використовувати будь-які платформи для контактів із вступником (за умов оприлюднення даних на офіційному сайті ЗВО). Ці заходи спрямовані на налагодження ефективної процедури проведення вступної кампанії до ЗВО в умовах карантину, забезпечення прав та свобод громадян на здобуття освіти.

Список використаної літератури:

1. Наказ МОН «Про затвердження умов прийому до закладів вищої освіти 2020 року» №1285 від 11.10.2019 р. Режим доступу: <https://mon.gov.ua/ua/osvita/visha-osvita/vstupna-kampaniya-2020/umovi-prijomu-do-vishih-navchalnih-zakladiv-v-2020-roci>.
2. Правила прийому до ВДПУ ім.М.Коцюбинського. Ел.ресурс. Режим доступу: <http://vspu.edu.ua/content/reception/vstup2020/dod/ruls.pdf>
3. Лист МОН № 1/9-228 від 30 квітня 2020 року «Щодо реєстрації на ЄВІ/ЄФВВ» Режим доступу: <https://mon.gov.ua/ua/news/rejestraciju-na-jevi-ta-yefvv-pereneseno-vona-vidbuvatimetsya-onlajn-list-mon>

Лапшин С.А.

кандидат історичних наук,
доцент кафедри правових наук та
філософії Вінницького державного
педагогічного університету
ім. М. Коцюбинського

Конотопенко О.П.

кандидат філософських наук,
доцент кафедри правових наук та
філософії Вінницького державного
педагогічного університету
ім. М. Коцюбинського

ОСОБЛИВОСТІ ПРОВЕДЕННЯ КОНКУРСУ НА ЗАМІЩЕННЯ ВАКАНТНИХ ПОСАД В ОРГАНАХ ВИКОНАВЧОЇ ВЛАДИ УКРАЇНИ У ПЕРІОД КАРАНТИНУ

Сучасна політична система України характеризується реформами які спрямовані на виправлення помилок попередників, стабілізації ситуації в країні та поліпшення репутації на міжнародній арені, адже з урахуванням нинішнього курсу України без всіх цих факторів євроінтеграція є неможливою. Однією з таких реформ стало оновлення апарату управління всіх рівнів [1]. Зрушення в даній сфері принесли за собою ряд нових питань, одним із таких став набір нових, молодих фахівців, так як галузь значно застаріла, і мислення її службовців значної мірою не відповідало потрібним вимогам [2]. Метою статті є аналіз особливостей проведення конкурсу на заміщення вакантних посад в органах виконавчої влади України у період карантину.

Порядок проведення конкурсу на посади державної служби здійснюється відповідно до вимог постанови Кабінету Міністрів: “Про затвердження Порядку проведення конкурсу на зайняття посад державної служби. Постанова Кабінету Міністрів України [4]; Порядок, Умови, Форма типового документа, Заява, Перелік від 25.03.2016 № 246”. Дана постанова визначає процедуру проведення конкурсу на зайняття вакантної посади державної служби (кон-

курс), метою якого є добір осіб, здатних професійно виконувати посадові обов'язки. Конкурс на зайняття посад фахівців з питань реформ проводиться за загальною процедурою з урахуванням особливостей, визначених даною постановою. Проведення конкурсу здійснюється відповідно до визначених в установленому законом порядку вимог до професійної компетентності кандидата на зайняття вакантної посади державної служби (посада) за результатами оцінювання його особистих досягнень, знань, умінь і навичок, моральних і ділових якостей для належного виконання посадових обов'язків.

Вимоги до професійної компетентності кандидата на зайняття посади включають кваліфікаційні вимоги, вимоги до компетентності та вимоги до професійних знань. Також слід зазначити що конкурс проводиться державною мовою. Конкурс проводиться з дотриманням принципів: 1) забезпечення рівного доступу; 2) політичної неупередженості; 3) законності; 4) довіри суспільства; 5) недискримінації; 6) прозорості; 7) доброчесності; 8) надійності та відповідності методів тестування; 9) узгодженості застосування методів тестування; 10) ефективного і справедливого процесу відбору.

Проведення конкурсу розпочинається з оголошення самого конкурсу на посаду, це роблять суб'єкт призначення (к. "А") або керівник державної (к. "Б" і "В") служби, в залежності від того під яку категорію підпадає посада (посади) оголошені на конкурс. Конкурс проводиться такими етапами: 1) прийняття рішення про оголошення конкурсу; 2) оприлюднення оголошення про проведення конкурсу; 3) прийняття та розгляд інформації від осіб, які бажають взяти участь у конкурсі; 4) проведення тестування та визначення його результатів; 5) розв'язання ситуаційних завдань та визначення їх результатів (у випадках, передбачених цим Порядком); 6) проведення співбесіди та визначення її результатів; 7) складання загального рейтингу кандидатів; 8) визначення суб'єктом призначення або керівником державної служби переможця (переможців) конкурсу; 9) оприлюднення результатів конкурсу.

Призначення на посаду державної служби відбувається у відповідному порядку згідно до статті 31 Закону України "Про державну

службу”. Щодо самого механізму призначення, виділимо чинники призначення на посаду в державній службі :

На посаду, на яку був оголошений конкурс державної служби призначається переможець конкурсу.

Рішення про призначення приймається: для посад державної служби категорії „А” – суб’єктом призначення, визначеним Конституцією та законами України; для посад державної служби категорії „Б” – керівником державної служби в державних органах, або відповідним суб’єктом призначення; для інших посад державної служби категорій „Б” і „В” – керівником державної служби, якщо інше не передбачено законом.

На посаду державної служби призначається особа, визначена переможцем конкурсу [3].

Рішення про призначення на посаду державної служби приймається суб’єктом призначення після проведення співбесіди з кандидатом та підписання з ним контракту про проходження державної служби (у разі укладення). Таке рішення приймається не пізніше п’яти календарних днів з дня надходження результатів спеціальної перевірки у випадку та порядку, передбачених законодавством у сфері запобігання корупції.

У разі встановлення за результатами спеціальної перевірки відомостей про претендента на посаду, які не відповідають встановленим законодавством вимогам для зайняття посади, приймається рішення про відмову у призначенні на посаду державної служби. Якщо особа не підписала контракт про проходження державної служби (причини можуть бути найрізноманітнішими) вона вважається такою, що відмовилася від зайняття посади державної служби. У такому разі застосовується відкладене право суб’єкта призначення на повторне визначення переможця конкурсу.

Якщо особа підписала контракт то служба управління персоналом у день призначення особи на посаду державної служби організовує складення Присяги державного службовця особою, яка вперше призначена на посаду державної служби, а також ознайомлює державного службовця під підпис з правилами внутрішнього службового розпорядку та посадовою інструкцією.

На початку 2020 р. пандемія коронавірусу торкнулася усіх сфер української держави. Запровадження карантину, обмеження соціальних комунікацій, дистанційна форма роботи інститутів державної влади викликали необхідність внесення змін до процедури проведення конкурсу на вакантні посади державної служби.

Докладніше проаналізуємо вимоги постанови Кабінету міністрів України «Порядок призначення на посади державної служби на період дії карантину, встановленого з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2».

Добір і призначення осіб на вакантні посади державної служби відповідно до цього Порядку здійснюється у виняткових випадках, пов'язаних з необхідністю виконання завдань і функцій державних органів на період дії карантину. Для призначення на посади державної служби суб'єктом призначення або керівником державної служби в державному органі першочергово розглядаються кандидатури, запропоновані Комісією з питань вищого корпусу державної служби (далі – Комісія) або конкурсною комісією, утвореною керівником державної служби у державному органі (далі – конкурсна комісія), за результатами процедур конкурсного відбору, зокрема у разі, коли строк оприлюднення результатів конкурсу перевищує 45 календарних днів з дня оприлюднення інформації про проведення такого конкурсу.

З метою визначення переможця (переможців) за результатами процедур конкурсного відбору проводиться співбесіда з кожним кандидатом, визначеним Комісією або конкурсною комісією:

на зайняття посад категорії “А” та посад категорії “Б”, які здійснюють повноваження керівників державної служби в державних органах, – суб'єктом призначення;

на зайняття інших посад категорій “Б” і “В” – керівником державної служби в державному органі.

Суб'єкт призначення або керівник державної служби в державному органі проводить співбесіду з кандидатами, в тому числі дистанційно в режимі відеоконференції за умови наявності технічної можливості.

Після проведення співбесіди суб'єкт призначення або керівник державної служби в державному органі приймає рішення про визначення переможця (переможців) за результатами процедур конкурсного відбору або про його (їх) відсутність.

На Єдиному порталі вакансій державної служби оприлюднюється інформація про: переможця (переможців) за результатами процедур конкурсного відбору; відсутність переможця за результатами процедур конкурсного відбору.

У разі відсутності або відхилення суб'єктом призначення або керівником державної служби в державному органі кандидатур, запропонованих Комісією або конкурсною комісією за результатами процедур конкурсного відбору, у порядку, передбаченому пунктами 3–10 цього Порядку, суб'єкт призначення або керівник державної служби в державному органі може призначити на посаду державної служби особу шляхом укладення контракту про проходження державної служби на період дії карантину та до дня визначення суб'єктом призначення або керівником державної служби в державному органі переможця конкурсу.

Призначення на такі посади здійснюється шляхом проведення співбесіди з визначеними суб'єктом призначення або керівником державної служби у державному органі посадовими особами [5].

Таким чином, функціонування апарату державної служби в Україні базується на конституційно-законних засадах та чітко керується своєю нормативно-правовою базою. Аспект вступу на державну службу та заміщення вакантних посад відповідає міжнародним нормам, що дає змогу переймати досвід зарубіжних колег.

Наявність чітко врегульованого, та відкритого процесу вступу на вакантні посади, дає змогу зрозуміти принципи проходження конкурсу, та в подальшому його оптимізації задля ефективного набору перспективних кандидатів, в приклад одного з таких можливих покращень можна привести наше невелике дослідження.

Характеризуючи питання конкурсного відбору то можна узагальнити: основними та незмінними вимогами до кандидатів на заміщення посад є відповідна освіта та досвід, але крім цих двох є

ще спеціальні вимоги, які можуть бути унікальними для кожного органу або структури, в залежності від посади та рангу. Такі особливі умови керуються відповідним наказом Національного агентства України з питань державної служби.

Проведення конкурсу базується на засадах законності та рівності для всіх кандидатів, так як це необхідні елементи для справедливого відбору кандидатів. Це надзвичайно важливий момент, тому що на етапі проведення конкурсу та відбору, кандидат на вакантну посаду показує свої професійні здібності. Але не дивлячись на те що цей порядок конкурсу затверджений Кабінетом Міністрів, на нашу думку він не є досконалим. Головною проблемою ми бачимо те що при конкурсі, відборі та призначення кандидатів на посаду не враховується момент психології даної людини, єдиним запобіжником від такої проблеми є проходження співбесіди, але вона не дає потрібного рівня захисту посад від потенційно некомпетентних осіб. Будь-який тест можливо пройти добре підготувавшись, будь-яка співбесіда може бути пройдена якщо наперед знати що від вас потребують. Тому на нашу думку варто ввести ще декілька запобіжних засобів, які визначали би психічні нахили людини, визначали б поріг моральності та компетентності кандидата. На нашу думку дані допоміжні етапи дозволили б розділяти та групувати людей на колективи, які в свою чергу назначались відповідно до підходящого виду зайнятості, виявляти схильності працівників та застосовувати їх за для покращення якості роботи на посадах державної служби, ми вважаємо таку тактику необхідною для досягнення найвищих результатів.

Список використаної літератури:

1. Новий курс: реформи в Україні 2010-2015. Національна доповідь / за заг. ред. В. М. Гейця (та ін.). - К. : НВЦ НБУВ, 2010. -С. 34.
2. Державна служба: підручник : у 2 т. / Нац. акад. держ. упр. при Президенті України ; редкол. : Ю. В. Ковбасюк (голова), О. Ю. Оболенський (заст.голови), С. М. Серьогін (заст. голови) [та ін.]. - К. ; Одеса : НАДУ, 2012. - Т. 1. -372 с.
3. Про державну службу: Закон України від 10.12.2015 р. № 889-VIII.

4. Постанова Кабінету Міністрів України: Про затвердження порядку проведення конкурсу на зайняття посад державної служби. Порядок, Умови, Форма типового документа, Заява, Перелік від 25.03.2016 № 246.

5. Постанова Кабінету міністрів України «Деякі питання призначення на посади державної служби на період дії карантину, установленого з метою запобігання поширенню на території України гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2» від 22 квітня 2020 р. № 290. Режим доступу: <https://www.kmu.gov.ua/npas/deyaki-pitannya-priznachennya-na-posadi-derzhavnoyi-sluzhbi-na-period-diyi-karantinu-ustanovlenogot220420>

СТОРІНКА МОЛОДОГО ВЧЕНОГО

Безкорвайна Н.М.

магістр, КНУ імені Тараса Шевченка

Науковий керівник:

Яременко О.І.,

кандидат наук з державного управління,
доцент

ПЕРЕДУМОВИ ЗАСТОСУВАННЯ ДЕРЖАВНО-ПРИВАТНОГО ПАРТНЕРСТВА У СФЕРІ КІБЕРБЕЗПЕКИ НА МІСЦЕВОМУ РІВНІ

У сучасному світі кількість кіберзагроз збільшується, вони стають краще організованими і більш складними. Для ризиків кібербезпеки характерна невизначеність щодо фізичного місця, суб'єктів, сфер життя тощо, що є викликом для управління ними та вимагає нових способів організації політики безпеки. Шляхом підвищення ефективності кіберзахисту є застосування органами місцевого самоврядування (далі – ОМС) моделі державно-приватного партнерства у цій сфері.

З огляду на триваючий процес децентралізації публічної влади в Україні, значення забезпечення кібербезпеки у сфері функціонування ОМС зростає. Як і органи державної влади, ОМС України демонструють неготовність ефективно протидіяти кіберзагрозам і мінімізувати їх негативні наслідки. Зокрема, сервісні системи Київської та Львівської міських рад стали об'єктами кібератаки версії вірусу Wannacry – Petya.A у 2017 році. Зазначене зумовлює актуальність пошуку нових шляхів вдосконалення механізмів забезпечення кібербезпеки країни, в тому числі на рівні територіальних громад.

Ведучи мову про кібербезпеку на місцевому рівні, слід розуміти її у широкому сенсі, як умови захищеності від фізичних, духовних, фінансових, політичних, емоційних, професійних, психологічних, освітніх або інших типів впливів або наслідків аварій, пошкоджен-

ня, помилки, нещасного випадку, шкоди або будь-якої іншої події в кіберпросторі, які могли б вважатися не бажаними [1, с. 66]. На сьогодні відсутні національні стандарти кібербезпеки для ОМС. Незважаючи на це, ОМС повинні почати розробляти власні стандарти кібербезпеки та впровадження проектів державно-приватного партнерства із консультаційною підтримкою від державних органів.

Основи законодавства у сфері кібербезпеки закладені у Законі України «Про основні засади забезпечення кібербезпеки України» (далі – Закон про кібербезпеку) [2]. Згідно статті 5 цього Закону органи місцевого самоврядування є одним із суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Суб'єкти забезпечення кібербезпеки у межах своєї компетенції: 1) здійснюють заходи щодо запобігання використанню кіберпростору у воєнних, розвідувально-підливних, терористичних та інших протиправних і злочинних цілях; 2) здійснюють виявлення і реагування на кіберінциденти та кібератаки, усунення їх наслідків; 3) здійснюють інформаційний обмін щодо реалізованих та потенційних кіберзагроз; 4) розробляють і реалізують запобіжні, організаційні, освітні та інші заходи у сфері кібербезпеки, кібероборони та кіберзахисту; 5) забезпечують проведення аудиту інформаційної безпеки, у тому числі на підпорядкованих об'єктах та об'єктах, що належать до сфери їх управління; 6) здійснюють інші заходи із забезпечення розвитку та безпеки кіберпростору (частина 5 статті 5 Закону про кібербезпеку).

У Законі про кібербезпеку для позначення співпраці державного і приватного сектору застосовується термін «державно-приватна взаємодія». Так, до принципів забезпечення кібербезпеки віднесений принцип державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері (стаття 7 Закону про кібербезпеку). Стаття 10 Закону про кібербезпеку визначає шляхи державно-приватної взаємодії у сфері кібербезпеки, проте вони не конкретизовані і мають описовий характер. Крім того, вживаючи

термін «державно-приватна взаємодія» закон не конкретизує, чи є така взаємодія державно-приватним партнерством (далі – ДПП) відповідно до термінології законодавства.

Функціонування ДПП в Україні регулюється Законом України «Про державно-приватне партнерство» (далі – Закон про ДПП) [3]. Державним партнером у договорі, укладеному в рамках державно-приватного партнерства, можуть виступати в тому числі органи місцевого самоврядування. У статті 4 визначені сфери застосування ДПП, серед яких відсутня сфера інформаційної безпеки або кібербезпеки. Відтак, не зрозуміло чи повинно партнерство у цій сфері регулюватися нормами цього закону. З огляду на зміст статті 10 Закону про кібербезпеку видається, що поняття державно-приватної взаємодії є ширшим і може включати також співпрацю на основі ДПП. Така невизначеність термінології не сприяє формуванню чіткості правового регулювання ДПП у сфері кібербезпеки і повинна бути усунута. Як вірно відмічають науковці, успішне державно-приватне партнерство може ґрунтуватися або на спільних інтересах або ж, якщо інтереси партнерів не збігаються, на чітких законодавчо закріплених вимогах [4].

За загальним розумінням ДПП є довгостроковою угодою між органом публічної влади та приватною компанією, на підставі якої приватна компанія адмініструє деякі послуги, які зазвичай належать до компетенції органів державної влади. Таке партнерство є раціональним за умови, якщо суб'єкт приватного сектору володіє необхідними ресурсами і здатний запропонувати краще співвідношення ціни та якості. Забезпечення кібербезпеки на основі ДПП передбачає залучення суб'єктів приватного сектору, а саме виробників серверного обладнання, розробників програмних продуктів і суб'єктів, що використовують елементи критичної інфраструктури, які залежать від інформаційно-комунікаційних технологій. Важливими для співпраці є відносини, пов'язані з розкриттям конфіденційної, комерційної та персональної інформації, досягнення співвідношення інтересів партнерів, розробка контрольних та наглядових процедур [7, с. 57]

Представляється неможливим підтримувати стабільні системи кібербезпеки без участі приватного сектору. Передумовами необ-

хідності впровадження ДПП є зростаюча складність власне технічного середовища, найму кваліфікованих кандидатів, особливо для ІТ-операцій. Ефективність ДПП, в тому числі у сфері інформаційної безпеки, доведена досвідом багатьох держав світу. Особливе значення така форма співпраці має для ОМС з огляду на обмеженість ресурсів. Так, у Польщі поширеність такої моделі співпраці найвища саме на місцевому рівні – воєводств, повітів та гмін, і зменшується на рівні центральних органів державної влади [5].

Втім, універсальної моделі успішного ДПП не існує; те, що ідеально працює в одній країні, може бути не придатне для функціонування в іншій. В основі меж застосування ДПП лежить поняття суспільного блага. Така взаємодія повинна мати безпосередній вплив на розвиток усього суспільства, а обидва сектори співпрацюють для досягнення спільної мети. Відповідно, такі межі у конкретній державі визначаються історичними, культурними, економічними та іншими факторами. На практиці такі ініціативи набувають найрізноманітніших форм. Визначальним є рівень розвитку відносин, які склалися між державним та приватним сектором у державі. В Україні він залишається низьким.

Для розуміння моделі побудови ДПП у сфері кібербезпеки на рівні ОМС в Україні слід розглянути підходи, які застосовуються у світі. Агентство Європейського Союзу з питань мережевої та інформаційної безпеки (ENISA) виділяє 4 моделі [6]. По-перше, модель інституційного ДПП. В її межах вся установа працює в рамках ДПП і надає багато послуг (дослідження, аудит безпеки тощо). Цей тип ДПП зазвичай пов'язаний із захистом критичної інфраструктури, а забезпечення кібербезпеки є одним із завдань. Формами співпраці є робочі групи, групи швидкого реагування та довгострокові об'єднання.

Другою є модель цілеорієнтованого ДПП, метою якою є формування культури кібербезпеки. Впровадження саме такої моделі на разі є актуальною для України. Формами співпраці є певна платформа чи рада, яка об'єднує приватний та державний сектор для обміну знаннями та найкращою практикою, де учасники фокусуються на одному предметі чи конкретній меті. Прикладом такого ДПП, яке включає також орган місцевого самоврядування як суб'єкта співпраці, є AEI Ciberseguridad y Tecnologías Avanzadas в

Іспанії в межах територіальної юрисдикції місцевого уряду Кастилії та Леона. Це асоціація, яка вже має майже сотню партнерів, і сприяє розробці системи безпеки інформації і технологій.

Третя модель – це сервісний аутсорсинг, який може ініціюватися урядом чи приватним сектором для підвищення рівня обізнаності про кібербезпеку серед зацікавлених сторін. Такі структури можуть сприяти впровадженню певних стандартів кібербезпеки чи підготовці національних стратегій кібербезпеки. Останньою моделлю є гібридне ДПП, яке передбачає поєднання елементів інституційної та аутсорсингової моделі ДПП. Частіше за все така діяльність пов'язана із функціонуванням CSIRT[6].

Таким чином, характеризувати ДПП у сфері кібербезпеки можна через такі аспекти, як структура управління та зміст. Структура управління охоплює організаційні питання, фінансові питання та правила спільної роботи. В літературі [4], як правило, ведуть мову про два типи управління: ієрархічне та горизонтальне. За першої моделі саме ОМС як представники публічної влади визначатимуть вимоги та завдання співпраці. За другоготипу управління ОМС та суб'єкти приватного сектору спільно формують проблему та розробляють порядок її вирішення.

Зміст ДПП у сфері кібербезпеки охоплює цілі партнерства та послуги, які спрямовані на їх досягнення. Досвід європейських країн найчастіше передбачає такі напрямки останніх: запобігання злочинності та шахрайству у кіберсфері; сертифікація та акредитація кібербезпеки; підключення та співпраця організацій з кібербезпеки; сприяння розширенню обізнаності та розуміння кібербезпеки серед громадян; ініціативи, спрямовані на надання можливості більшій кількості людей стати професіоналами з кібербезпеки; проведення досліджень та науково-технічних розробок у сфері кібербезпеки. Деталізація таких послуг заснована на типах загроз кібербезпеці, які пов'язані із повноваженнями, якими наділені ОМС. Тому особливе значення має розробка стратегії розвитку територіальної громади із визначенням пріоритетних напрямків розвитку у сфері інформаційної безпеки. Важливо розуміти, що ОМС не може передавати відповідальність за кібербезпеку. За ДПП делегується лише саме функціонування такої послуги.

На заваді побудови цілісної системи кібербезпеки в Україні стоїть також обмеженість даних про стан українського кібербезпечного сектору – не лише в аспекті інформування суспільства та фахівців, але й часто щодо самих суб'єктів забезпечення кібербезпеки держави[8, с. 67-68]. Зазначене призводить до браку довіри між суб'єктами-потенційними учасниками ДПП у сфері кібербезпеки. Це притаманно і системі ОМС: вони не володіють достатньою інформацією про наявні ресурси і способи та можливості у цій сфері. З огляду на це, доцільно запроваджувати конкретні невеликі проекти без суперечності інтересів і які не вимагають залучення значних ресурсів ОМС задля формування довіри до таких органів і накопичення відповідного досвіду для уникнення ризиків у майбутньому. Тому до передумов застосування ДПП на місцевому рівні слід віднести визначення таких проектів, зокрема, вони можуть стосуватися реалізації спільних наукових та дослідницьких проектів. Перевагами є те, що приватна компанія може не лише постачати свої технології та надавати експертів для їх створення, але і залучати та навчати працівників ОМС. Вони набувають навичок, які згодом можуть бути використані на користь інших секторів управління.

Таким чином, під ДПП у сфері кібербезпеки на місцевому рівні слід розуміти співробітництво між органами місцевого самоврядування та суб'єктами приватного сектору з метою зменшення ризиків кібербезпеки шляхом посилення можливостей кіберзахисту, співпраці та обміну інформацією. Створення сприятливих умов для розвитку ДПП на місцевому рівні передбачає, перш за все: визначення стратегії розвитку територіальної громади із пріоритетними напрямками у сфері кібербезпеки та взаємодії ОМС і приватного сектору у цій сфері; узгодження термінів «державно-приватна взаємодія» і «державно-приватне партнерство» у законодавстві; конкретизацію шляхів державно-приватної взаємодії у сфері кібербезпеки у статті 10 Закону України «Про основні засади забезпечення кібербезпеки України»; закріплення принципів взаємовідносин ДПП місцевого рівня у сфері кібербезпеки; доповнення переліку сфер застосування ДПП у статті 4 Закону України «Про державно-приватне партнерство» сферою кібербезпеки. До інституційних передумов застосування ДПП слід віднести створення у

межах ОМС спеціальної структурної одиниці (підрозділ, комісія тощо), до якої будуть входити фахівці із відповідними набором знань і досвіду у сфері ІКТ, та наділення їх повноваженнями підготовки і реалізації проектів ДПП у сфері кібербезпеки.

Література:

1. Шеломенцев, В. П. Кібербезпека: поняття та сутність [Текст] / В. П. Шеломенцев // Моделювання колективної безпеки: інформаційний вимір : матеріали міжнар. круглого столу, 27 квіт. 2011 р. К. : НДЦ правової інф-ки НАПрН України, 2011. С. 66-67
2. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: <http://zakon.rada.gov.ua/laws/show/2163-19>.
3. Про державно-приватне партнерство: Закон України від 1 липня 2010 року № 2404-VI. URL: <http://zakon.rada.gov.ua/laws/show/2404-17>
4. Carr M.. Public-private partnerships in national cyber-security strategies. International Affairs, 92(1),2016.C. 43-62
5. Herbst I., Jadach-Sepiolo A., Korczyński T. Raport o partnerstwie publiczno-prywatnym w Polsce / Praca zbiorowa pod redakcją prof. dr hab. Jerzego Hausnera. Warszawa, 2013. URL:https://www.nist.gov/pl/files/zalacznik/1452372455_ppp.pdf
6. Public Private Partnerships (PPP) Cooperative models.European Union Agency for Network and Information Security (ENISA), 2017. URL: https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models/at_download/fullReport
7. Круглов В.В. Державно приватне партнерство у сфері кібербезпеки. Вчені записки ТНУ ім. В.І. Вернадського. Серія: Державне управління. 2018. № 3, т. 29 (68). С. 57-61
8. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України: аналіт. доп. / за заг. ред. Д. Дубова. Київ: НІСД, 2018. 84 с.

Власова І.А.

здобувач СВО магістра,

Вінницький державний педагогічний
університет ім. М. Коцюбинського

ХАРАКТЕРИСТИКА ЗАРУБІЖНОГО ДОСВІДУ РЕФОРМУВАННЯ ПУБЛІЧНОГО УПРАВЛІННЯ: ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИЙ АСПЕКТ

Функціонування публічного управління є однією з найбільш гострих проблем українського суспільства через низьку ефективність політики розвитку адміністративно-територіальних одиниць у державі, неактивність публічної адміністрації відносно суспільних трансформацій, низьку якість публічних послуг та вкрай низький рівень довіри людей до органів влади.

Зарубіжний досвід реформування публічного управління є важливим засобом розв'язання зазначених проблем та має бути адаптованим до умов України, оскільки ідея реформування належним чином ще не відпрацьована законодавчо, а консервативні тенденції в управлінні, як наслідок тоталітарного минулого країни, залишаються сильними.

Даною проблемою на науковому рівні займалися ряд дослідників. Серед них: Грицяк І.А., Шереметьєва Л.А., Баранцева К.К. [1], Мельтюхова Н. М., Корженко В. В., Дідок Ю.В. [2], Мальковська І.А. [3].

Активна реалізація євроінтеграційних прагнень України неможлива без вивчення проблематики публічного управління та врахування зарубіжного досвіду. Європейські принципи визначаються Європейською Комісією як принципи європейського врядування та торкаються безпосередньо управлінської діяльності національних органів ЄС.

Варто звернути увагу та зупинитися на групі європейських принципів адміністративного права, адже саме ця група принципів призначена регулювати правовідносини між громадянами та органами влади у такий спосіб, аби захистити перших від перевищення повноважень чи свавілля других, прийняття прозорих та зрозумілих рішень на користь та в інтересах громадян, забезпечити ефективність управління.

Європейські принципи адміністративного права сформувалися на тлі конституційно-правових норм (захист прав людини, гарантія громадянських, політичних, соціальних прав і т. ін.) та узагальненні управлінської практики. Відповідно, вони мають подвійну – адміністративно-правову – природу [1, с. 8]

Наступну групу складають принципи, які безпосередньо торкаються управлінської діяльності наднаціональних органів ЄС, визначаються Європейською комісією як принципи європейського врядування [2].

За основу ефективного врядування взято п'ять принципів, визначених у Білій книзі Європейського врядування. Кожен принцип є важливим для більш демократичного врядування. Вони підтримують демократію та принцип верховенства права у державах-членах ЄС, але можуть бути застосовані на усіх рівнях влади – світовому, Європейському, національному, регіональному і місцевому:

- відкритість – інституції повинні працювати більш відкрито, активно обмінюватися інформацією з державами-членами ЄС, з приводу того, що робить ЄС, які рішення він приймає;

- участь – якість, релевантність та ефективність політики ЄС залежить від участі широкого кола осіб та організацій на всьому шляху творення політики – від її планування до впровадження;

- підзвітність – ролі у законодавчому та виконавчому процесах повинні бути більш зрозумілими, кожна з Інституцій ЄС повинна пояснювати і брати відповідальність за те, що вона робить для Європи;

- ефективність – політика має бути ефективною і своєчасною, такою, що забезпечує усе що потрібне на підставі чітких завдань, оцінки майбутнього впливу та попереднього досвіду;

- злагодженість – політика та усі заходи повинні відповідати один одному та бути легкозрозумілими, потреба у злагодженості постійно зростає внаслідок різноманітності, присутньої в ЄС [4, с. 11-12].

Отже, європейські принципи можна охарактеризувати як конституційні, на цих загальних принципах ґрунтуються сучасні демократії на всіх континентах світу. Між тим, до цієї категорії принципів належать: верховенство права, повага до прав та свобод людини, рівне ставлення, відсутність дискримінації.

Таким чином, проаналізувавши принципи європейського врядування та як вони визначені у Білій книзі з європейського врядування, маємо підстави стверджувати, що вони фактично є загальноновизнаними світовими принципами належного врядування.

Другу категорію принципів можна визначити як принципи належного врядування, які дають змогу державам або об'єднанням держав перетворити системи публічної адміністрації на більш ефективні та результативні, залучити до співробітництва як можна більше громадян, вдало конкурувати на товарних чи фінансових ринках.

До третьої категорії входять принципи, які характеризують європейське врядування як унікальну форму взаємодії між різними учасниками процесу прийняття управлінських рішень в ЄС, вироблення та реалізації європейських політик на різних рівнях, а саме: наднаціональному, національному, субнаціональному.

До четвертої категорії принципів європейського врядування можна віднести принципи, на яких базуються окремі спільні політики чи програми ЄС, наприклад забезпечення права громадян ЄС на повну та не викривлену інформацію, пристосування Європейської комунікативної політики, її повідомлень та сигналів до національних, регіональних чи місцевих потреб.

Слід зазначити, що в умовах європейського врядування зростає роль комунікацій, саме надання та поширення інформації є першим кроком для досягнення взаєморозуміння, для вироблення спільної позиції.

Крім цього, чим інтенсивніше взаємодія, тим активніше відбувається обмін інформацією, тим важливішими стають навички спілкування.

В системі європейського врядування однаково важлива формальна й неформальна комунікація. На важливості першої наголошують комунікативна політика ЄС [1], комунікативні політики держав-членів, щодо неформальної – міжособистісної – комунікації особливого значення набуває міжкультурна комунікація [3].

Крім цього, на сьогоднішній день більшість зарубіжних країн звертаються до інформаційно-комунікаційних технологій (ІКТ) для модернізації державного управління. Формуючи нові цінності,

політичні та соціальні пріоритети, нові форми участі громадянського суспільства в управлінні державою, інформаційне суспільство має величезний економічний потенціал.

Питання свободи інформації досить чітко прописано у Конвенції Ради Європи про доступ до офіційних документів, а саме: державні організації зобов'язані розкривати інформацію, якщо жоден член суспільства не має відповідне право отримувати інформацію; кожна особа, присутня на території країни, повинна користуватися цим правом; кожна особа має право на свободу інформації, включаючи право доступу до інформації, яка знаходиться в розпорядженні державних органів, лише за умови дотримання положень Закону [5].

Так, у квітні 2018 року Україна підписала Конвенцію Ради Європи про доступ до офіційних документів (Конвенцію Тромсо). Це перший міжнародний документ у якому держави не лише визнають право на доступ інформації, а й погоджуються забезпечувати таке право і співпрацювати у сфері доступу.

Однак, на даний час Конвенція Ради Європи про доступ до офіційних документів не ратифікована Україною.

Таким чином, зарубіжний досвід публічного управління вказує на значну вагу в ньому інформаційного суспільства. Забезпечення комунікації та свобода інформації, доступ до неї є неодмінними рисами організації державного управління в країнах Європейського Союзу. Інформаційні-комунікаційні технології сприймаються як форми та засоби модернізації державного управління. Вважаємо, що цей досвід неодмінно повинен бути оцінений та використаний під час реформ державного управління в Україні.

Список використаної літератури:

1. Зарубіжний досвід державного управління: доцільність і можливість застосування в Україні: наук. розробка / авт. кол.: І. А. Грицяк, Л. А. Шереметьєва, К. К. Баранцева та ін. – К. : НАДУ, 2012. – 56 с.
2. Зарубіжний досвід публічного адміністрування: методичні рекомендації / Н. М. Мельтюхова, В. В. Корженко, Ю. В. Дідок та ін. – К.: НАДХ, 2010. – 28 с.
3. Мальковская И. А. Трансформация государства и эволюция публичного администрирования в условиях глобализа-

ции / И. А. Мальковская. // Вестник Российского университета дружбы народов. Серия: политология. – 2006. – № 8. – С. 27-43. – Режим доступа: <https://cyberleninka.ru/article/n/transformatsiya-gosudarstva-i-evolyutsiya-publichnogo-administrirovaniya-v-usloviyah-globalizatsii-aktualizatsiya-evropeyskogo/viewer>.

4. Європейське врядування. Біла книга. – Режим доступу: https://pravo.org.ua/files/konstatyts/WHITE_BOOK_UKR_REV.pdf.

5. «Конвенція про доступ до офіційних документів» від 18 червня 2009 р. // Центр демократії та верховенства права. – Режим доступу: <https://cedem.org.ua/library/konventsia-rady-yevropy-pro-dostup-do-ofitsijnyh-dokumentiv-ofitsijnyj-pereklad/>

Добжанська М.Є.

студентка освітньо-кваліфікаційно-
го рівня магістра Вінницького дер-
жавного педагогічного університету
ім. М. Коцюбинського

ІНФОРМАЦІЙНА СКЛАДОВА УПРАВЛІННЯ СФЕРОЮ КУЛЬТУРИ: МІЖНАРОДНІ ВІДНОСИНИ

Специфіка національних культур викликана багатьма обставинами та факторами. Національні культури протягом декількох тисячоліть розвивались автономно одна від одної. Це пояснювалось відсутністю тривалий час засобів масової комунікації, через що інтенсивне спілкування між народами було неможливим. Внаслідок цього сформувалося певне відособлення у розвитку культури різних націй, вони отримали окремі системи цінностей, що визначають їхню оригінальну ментальність та специфічність духовного розвитку.

Однією з головних складових державної інформаційної політики нині є інформаційна культура, як особистості так і суспільства – феномен, який виник упродовж останніх кількох десятиліть під еволюційним впливом розвитку соціокультурного середовища. Поняттям «інформаційної культури» оперує велика кількість галузей науки, вивчаючи різноманітні її аспекти, зумовлюючи тим самим відсутність єдиних, усталених підходів до його трактування.

Досі залишається предметом дискусій у науці, дослідження інформаційної складової сфери культури як науково-теоретичної проблеми в сучасних умовах розвитку держави, подальший розвиток міжнародних відносин за нових соціально-економічних та культурних умов розвитку суспільства.

Слова «інформаційна культура» – латинського походження, де «cultura» – освіта, розвиток та «informatio» – роз'яснення – це: множина досягнень певного людського суспільства (групи людей, нації, народу, суспільства, держави, міжнародного співтовариства) у сфері інформаційних відносин (у тому числі мистецтва, науки, техніки тощо); відповідний рівень розвитку інформаційних відносин на певний момент часу, у просторі, колі осіб, що визначається

порівняно з попередніми показниками інформаційної культури; множина практичних, матеріальних і духовних надбань суспільства, які відображають історично досягнутий рівень його розвитку у сфері інформаційних відносин та втілюються в результатах інформаційної діяльності.

У своїх працях, багато визначних науковців розглядають динамічні соціально-культурні процеси: В. Степанов, П. Клімушин, О. Валецький, В. Паращук, М. Закович, Т. Коломієць, Г. Купряшин, В. Чернець, Л. Максим'як, І. Маслікова, О. Семеченко, Г. Скрипчук, О. Снісаренко та інші.

Відомі політологи розглядають культуру як чинник соціально-економічного розвитку суспільства: Я. П'єтрась, С. Хантингтон, С. Верба, Г. Алмонд, виокремлюють політологічне розуміння культури орієнтує на конкретний аналіз політичних систем, що базується на виявленні культурних кодів, які історично сформували смислові системи, що виконують функцію спрямування соціальних і політичних процесів.

Концепція, де однією з ланок, що об'єднує всю суспільну систему, є людина, котра водночас виступає як суб'єктом, так і об'єктом соціальних інтересів, потреб та духовно-моральних цінностей, ідеалів, прагнень і переконань. Безпосередній вплив на поведінку й діяльність людини, мають пов'язані з інформаційною сферою моральні цінності. Саме вони формують усю систему її індивідуально-суспільних відносин. Людина як найвища соціальна цінність акумулює в основних формах своєї життєдіяльності й інформаційно фіксує взаємозв'язок духовного й матеріального, відображаючи в цілісному вигляді життя як об'єктивну реальність, де виявляються її внутрішньо взаємозалежні інтереси, моральні цінності, ідеали, її культура, релігійні вподобання та суб'єктивне розуміння сенсу життя. Суспільство стає тією універсальною матеріально-духовною сферою, в якій особистість може реалізувати себе цілісно. Справедливо зазначає О. Дзьобань, що із соціально-економічними та політичними трансформаціями інформаційного суспільства відбувається процес переоцінки духовних цінностей, формування принципово нових засад моралі.

Видатний американський політолог С. Хантингтон, зазначає, що зразки спільностей та дезінтеграцію і конфлікти у світі, після холод-

ної війни, визначають культура і культурна ідентичність. Прогрес національних культур впродовж тисячоліть формувався автономно одна від одної, що пояснюється відсутністю в минулому засобів масової інформації не тільки у глобальному, а й регіональному масштабах. Як наслідок відносного відособлення культурного розвитку різних народів світу, кожна культура склалась як окрема система цінностей, що дає визначення для світогляду. Специфічність розвитку культури і мистецтва, є основою для виникнення та прогресу релігійних та ідеологічних систем. Політолог С. Хантингтон, розглядає світ через призму цивілізацій що, на думку науковця, відповідають просторам: західну, православну, ісламську, латиноамериканську, індуїстську, буддистську, китайську, японську та африканську цивілізації.

Нестримний розвиток міжнародного культурного середовища дає поштовх для розвитку найрізноманітніших культурних просторів, які класифікуються по різному. У політико-режимному підході можна виокремити демократичний (США, Канада, Японія, Європейський Союз), авторитарний (Арабський світ, Китай, Венесуела, Куба, переважна більшість країн СНД та ін.), тоталітарний (Північна Корея, Іран) та транзитивний (перехідний) (Україна, деякі країни Латинської Америки, Молдова, Грузія тощо) простори культури.

Континентальний підхід до стратифікації політичної культури, який розробили американські політологи С.Верба і Г. Алмонд, розподілити основні країни світу за наступними типами:

1. Англо-американський тип політичної культури (США, Велика Британія, Канада, Нова Зеландія, Австралія), що характеризується розумінням політики, як процесу зіткнення інтересів, які завжди можна примирити, тяжіння електорату до політичного центру. Світським, прагматичним характером.

2. Континентально-європейський тип політичної культури (Німеччина, Франція, Австрія, Іспанія, Італія, Бельгія та ін.) характеризується багатопартійно-поляризованим спектром.

3. Авторитарно-патріархальний тип політичної культури. Характеризується архетипом «великої родини» на чолі з традиційно авторитарним лідером (це авторитарні суспільства в ряді країн Азії, Латинської Америки, Африки).

4. Тоталітарна політична культура – де існує повний контроль влади за політикою і культурою (Іран, Північна Корея).

Інформаційна сфера є важливою складовою міжнародного життя з найдавніших часів до сучасності. Прогресія сучасних інформаційних та комунікаційних технологій визначають динаміку розвитку у внутрішній та зовнішній політиці держав. Для дослідження сутності сучасного інформаційного суспільства необхідно визначити склад і структуру знань, навичок і умінь, що визначають інформаційну культуру особистості.

Цікавою є точка зору Н. Семенюк, згідно з якою інформаційна культура особистості як умова успішної адаптації людини до життя в інформаційному суспільстві еволюціонує в суспільство знань. У новій парадигмі освіти, зазначає Н. Семенюк, значне місце займає інформаційна складова, яка має принципово важливе значення як для тих, хто вчить, так і для тих, хто навчається. Відповідно в останні роки в усьому світі серйозну увагу почали приділяти інформаційній підготовці особистості. Ця підготовка повинна орієнтуватися не тільки на навчання прийомам раціональної роботи з книгою, ліквідації комп'ютерної неграмотності, алгоритмам інформаційного пошуку, освоєнню гіпертекстових, мультимедійних та інших інформаційно-комунікаційних технологій. У цьому контексті Н. Семенюк виокремлює твердження стосовно необхідності цілеспрямованої й комплексної підготовки людини, що включає широкий спектр інформаційних знань, умінь і навичок, інформаційних компетенцій, що пов'язані із пошуком, вилученням та критичним аналізом інформації, здатність самостійно добувати і виробляти нові знання. Саме інформаційний світогляд є важливою ланкою, що поєднує всі компоненти інформаційної культури. «Інформаційний світогляд» – система узагальнених поглядів на інформацію, інформаційні ресурси, інформаційні технології, інформаційні системи, інформатизацію, інформаційне суспільство та місце людини в ньому, ставлення людей до навколишнього інформаційного середовища, а також обумовлені цими поглядами їх ідеали, переконання, принципи діяльності і пізнання нового.

Міжнародний інформаційний простір визначається як: система середовища буття людини, яка забезпечує діяльність будь-якої системи, зокрема – системи міжнародних відносин; система спільного використання національних інформаційних ресурсів за узго-

дженими сферами і напрямками діяльності; сума складних інформаційних технологій, які є основою і визначальним компонентом промислово-економічного комплексу транснаціональних спільнот, які впливають на формування світоглядних процесів у суспільстві.

У центр уваги розвитку висувається проблема формування інформаційної культури суспільства. Розвинена інформаційна сфера, інформаційно-комунікаційні технології, виступають запорукою соціального, економічного і політичного благополуччя. Численні наукові праці, які присвячені інформаційній ері, здебільшого виокремлюють, що змінюються не тільки технологічна база й інформаційно-технологічні можливості людини, а й сама людина, її самосвідомість. Людина сучасності стає немислимою без інформаційних технологій, які справляють величезний вплив на все її існування – як соціальне, так і біологічне. При всій суперечності точок зору, практично всі вчені погоджуються в одному: особливу роль у сучасному світі й становленні нової людини відіграє інформаційна культура. Міжнародні відносини у інформаційній сфері пов'язані зі стосунками між її виробниками та споживачами щодо отримання останніми повідомлень про реальні події, що становлять для них інтерес. Споживачі інформації можуть використовувати її операційно, але також і для подальшого передавання іншим споживачам.

Реальний міжнародний порядок у сфері міжнародних інформаційних відносин визначається фінансовими і, відповідно, технічними можливостями кожної держави світу. Слушно вважають С. Дрожжина і І. Кобзар, сучасна інформаційна техніка може змінювати чи навіть руйнувати ціннісні пріоритети та життєвий світ людини у цілому, відволікати її від реалій життя, занурюючи у віртуальну реальність. Тобто в умовах інформаційного суспільства виникає новий спосіб існування культури – у віртуальній реальності [2].

Зафіксовані зміни у сфері духовної культури викликані безособовою логікою технічного розвитку, процесами самоорганізації техногенного середовища, а не свідомими діями її творця – людини. Інформаційні технології, наприклад, за допомогою структуризації інформації й забезпечення її доступності здійснюючи глибокі трансформації індивідуальної й масової свідомості, уніфікують

соціальні практики, забезпечують включення людей у глобальний інформаційний обмін, стають інструментом психологічного тиску, проти волі втручаючись в емоційно-вольову сферу людини. Такої ж думки дотримується й А. Алехнович, визначаючи, що відбувається «підрив екзистенційного улаштування присутності, оскільки екзистенціали турботи, страху, тривоги витісняються за межі рефлексії, елімінується переживання власного кінця та тимчасовості існування, приносячи заспокоєння й почуття безпеки; це світ позачасовості, точніше, сьогочасності – час онлайн, безпосереднє задоволення інформаційних потреб» [1].

Аналіз особливостей міжнародно-правових актах у досліджуваній сфері свідчить, що в них закріплено: а) визнання людини і громадянина повноправним суб'єктом інформаційних відносин, що виникають між ним і державою, що, у свою чергу, є необхідною умовою для формування інформаційної культури на загальнодержавному та індивідуальному рівнях, а також на рівні окремих соціальних інститутів; б) засади транскордонності в оволодінні здобутками інформаційної культури представників різних країн; в) етичні стандарти представників окремих сфер суспільних відносин (журналістів, державних службовців та ін.) як складова частина ціннісного рівня інформаційної культури; г) необхідність розвивати світоглядні, ціннісні, когнітивні, комунікативні та інструментальні компоненти інформаційної культури для формування більш демократичного і сталого інформаційного суспільства; ґ) розуміння інформаційно-комунікаційних технологій як інструменту для досягнення соціально-значущих цілей, а не самоцілі; д) необхідність приділяти особливу увагу інформаційним потребам і можливостям осіб з меншою соціальною захищеністю; е) комплексність підходу до компетенцій для навчання протягом життя, в системі яких вміння користуватися цифровими технологіями (пристроями) має поєднуватися з розвитком аналітичних, творчих та інших здібностей особистості.

Культура створення, обміну та споживання інформації стрімко зростає та поширюється. Людину необхідно підготувати до швидкого сприйняття й обробки великих обсягів інформації, до оволодіння нею сучасними засобами, методами і технологією роботи. Новітні умови роботи породжують залежність інформованості

однієї людини від інформації, набутої іншими людьми. Тому вже недостатньо вміти самостійно накопичувати інформацію, а необхідно опанувати таку технологію роботи з нею, коли готуються і приймаються рішення на основі колективного знання. Це говорить про те, що людина повинна мати певний рівень культури щодо поводження з інформацією.

Як висновок, слід підкреслити, що суспільство сучасності висуває низку вимог як до особистості стосовно рівня її інформаційної культури, так і міжнародного суспільства. Необхідні уміння адекватно формалізувати знання; адекватність інтерпретації формалізованих даних та використання нових інформаційних технологій у своїй життєдіяльності; спроможність ефективно використовувати сучасну комп'ютерну техніку та інформаційні технології, що сприяють формуванню парадигми інформаційної людини та нації. Фундаментальний суспільний інтерес у цьому контексті полягає у формуванні світоглядної культури, стрижнем якої стає інформаційна культура.

Література:

1. Алехнович А. С. Категорія екзистенціональної свідомостів системі гуманітарних наук [Електронний ресурс] / А. С. Алехнович. – Режим доступу: <http://www.zpu-journal.ru/e-zpu/2012/1>.
2. Губа А.В. Характеристика складових управлінської культури в світі / А.В. Губа // Педагогіка і психологія. Вісник Академії педагогічних наук України. – 2008. – № 3-4 (60-61). – С. 107-116.
3. Дрожжина С. В. Аксиологічно-екзистенційні детермінанти інформаційного суспільства / С. В. Дрожжина, І. М. Кобзар // Гілея : наук. вісн. : зб. наук. пр. / голов. ред. В. М. Вашкевич. – К. : Гілея, 2014. – Вип. 80 (1). – С. 190–196.
4. Копієвська О. Р. Всесвітня культурна спадщина: регулювання міжнародним правом / О. Р. Копієвська // Держава і право : зб. наук. пр. / Ін-т держави і права ім. В. М. Корецького НАН України. – К., 2006. – Вип. 33. Юрид. і політ. науки. – С. 25–30.
5. Каткова Т. Г. Поняття культурної спадщини за міжнародним та українським законодавством / Т. Г. Каткова // Право і безпека. – 2005. – Т. 4. – № 5. – С. 148–152.

Іванова А.В.

здобувач СВО магістра,
Вінницький державний педагогічний
університет ім. М. Коцюбинського

КАДРОВА БЕЗПЕКА В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ

В сучасних умовах кадровий потенціал держави, установи, організації та підприємства є необхідною умовою їх належного функціонування. «Кадри вирішують все» – відома формула епохи Перестройки, що проголошена М. Горбачовим, насправді була спробою нової інтерпретації тези тоталітарного лідера СРСР Й. Сталіна, проголошеної ним у 1935 р. разом із гаслом «Самий цінний капітал – це люди». Однією з причин розвалу Радянського Союзу, на нашу думку, став кадровий голод, насамперед, в економічних реформах, що з часом призвів до неефективного управління економічними процесами, швидкого зубожіння народу та наростання політичних негараздів. Проте ці тези є надзвичайно актуальними для України в сучасних умовах, оскільки, на нашу думку, саме брак кваліфікованих менеджерів – основна причина провалу різноманітних реформ в Україні. Кількість державних чиновників різного рівня збільшується з кожним роком, проте якість кадрового потенціалу досі залишається низькою. Питання забезпечення кадрової безпеки у державному управлінні сьогодні стоїть досить гостро.

Поняття кадрової безпеки піднімається багатьма вченими та дослідниками різних наук. Проте найчастіше, на нашу думку, воно лунає у працях економістів та політологів у контексті економічної чи політичної безпеки. Але сфера державного управління сьогодні як ніколи потребує сучасних менеджерів-управлінців, оскільки саме від них залежить ефективність та результативність системи державного управління. Дефініція «кадрова безпека» має декілька підходів, оскільки кожен із науковців вкладає у неї ті завдання, які повинні вирішувати кадри у різних суспільних сферах суспільного життя. Так, дослідниця О. Пархоменко-Куцевіл виділяє наступні підходи трактування поняття:

- процес запобігання негативним впливам на економіку через ризики і погрози, що пов'язані з його інтелектуальним потенціалом і трудовими відносинами;

- безбитковість трудових відносин підприємства, метою якої є досягнення максимальної стабільності функціонування фірми, а також створення основи і перспективи росту з метою виконання її основних завдань;

- генеральний напрямок кадрової роботи, сукупність принципів, методів, форм організаційного механізму з опрацювання цілей, завдань, спрямованих на збереження, зміцнення розвиток кадрового потенціалу, на створення відповідального і високопродуктивного згуртованого колективу, здатного вчасно реагувати на постійно мінливі вимоги ринку з урахуванням стратегії розвитку організації;

- правове та інформаційне забезпечення процесу управління персоналом: вирішення правових питань трудових відносин, підготовка нормативних документів, які їх регулюють, забезпечення необхідною інформацією всіх підрозділів управління персоналом, що скоріше є функціями кадрової безпеки підприємства;

- сукупність управлінських заходів, пов'язаних із ефективним формуванням та використанням кадрового потенціалу підприємства з метою забезпечення та підтримки економічної стійкості та результативності господарської діяльності підприємства;

- характеристика процесу функціонування економічної системи, за якого відбувається ефективне функціонування всіх її функціональних складових; забезпечення захищеності й здатності протистояти внутрішнім та зовнішнім впливам і загрозам, пов'язаним із персоналом; змістовний та структурний аналіз, діагностика й прогнозування впливу діяльності персоналу на внутрішні та зовнішні показники згаданої економічної системи [1, с. 14].

Автор пропонує розглядати кадрову безпеку у системі державного управління як «сукупність механізмів, методів, принципів, спрямованих на формування, розвиток та збереження кадрового потенціалу системи державного управління» [1, с. 14].

До цього часу бачимо домінування у трактуванні понять кадри, кадрова безпека, кадровий потенціал менеджменту як науки.

Однак, наука державного (публічного) управління сформувалася із економічного і соціального менеджменту. Саме тому Л. Калганов прямо вказує, що незважаючи на існуючі розбіжності між державним управлінням та менеджментом, останнім часом намітилася тенденція методологічного наближення цих сфер соціального управління, а методи та інструментарій менеджменту можна та необхідно використовувати в сфері державного управління з урахуванням його особливостей і спеціальних функцій [2, с. 58].

Дослідниця Н. Подлужна на прикладі конкретної державної установи показала, що кадровій безпеці у системі державного управління загрожують внутрішні та зовнішні чинники. До внутрішніх вона відносить високий рівень плинності кадрів, неефективну систему мотивації, недостатню кількість раціоналізаторських пропозицій і ініціатив, слабку організацію системи навчання. До зовнішніх: кращі умови праці у конкурентів та інфляційні процеси [3, с. 211].

Інші автори пропонують розглядати загрози кадровій безпеці залежно від можливості прогнозування: передбачувані або непередбачувані; залежно від об'єкта безпеки: кадри, технічне оснащення, інформація, технології, імідж; залежно від сфери виникнення: зовнішні та внутрішні[1, с. 15].

В умовах утвердження демократичних принципів управління державними процесами неодмінно постає питання удосконалення кадрової політики держави. Реалізація державної кадрової політики передбачає, насамперед, переорієнтацію державного управління із системоцентричної парадигми на персоноцентричну [4, с. 54]. Тобто в основі сучасної моделі державного управління має стати не чиновник-бюрократ як елемент певної системи, а менеджер-управлінець, що забезпечить ефективне функціонування моделі публічного управління.

Шляхами вдосконалення державної кадрової політики, а отже вдосконалення й кадрової безпеки можуть бути наступні кроки: профорієнтація, профвідбір, профпідготовка, профперепідготовка; розстановка і закріплення кадрів; удосконалення мотиваційного механізму їх діяльності; покращення умов і привабливості праці; профатестація, стимулювання професійного зростання; ро-

бота з резервом кадрів; контроль за діяльністю персоналу; система інформування кадрів про завдання колективів; виховання кадрів [4, с. 52].

О. Пархоменко-Куцевіл пропонує внутрішні та зовнішні механізми забезпечення кадрової політики в системі державного управління. До внутрішніх механізмів вона включає забезпечення захисту працівника в системі державного управління (охорона здоров'я, соціальний захист, правові гарантії); професійний розвиток фахівця в системі державного управління (адаптація, мотивація, навчання, підвищення кваліфікації, оцінювання). До зовнішніх – забезпечення формування єдиної кадрової політики щодо розвитку кадрів у системі державного управління; здійснення якісного відбору кадрів з метою формування кадрового складу системи державного управління [1, с. 15].

Ефективну систему забезпечення кадрової безпеки можливо забезпечити лише з утвердженням принципів державної служби в Україні, що запропоновані новим Законом України «Про державну службу в Україні від 10 грудня 2015 р. Так, він до основних принципів державної служби в Україні відносить принципи верховенства права, законності, професіоналізму, патріотизму, доброчесності, ефективності, забезпечення рівного доступу до державної служби, політичної неупередженості, прозорості, стабільності [5, с. 43].

Важливу роль у забезпеченні кадрової безпеки в сучасних умовах покладається на кадрові служби органів державної влади та органів місцевого самоврядування. Організація кадрової роботи, її планування, передбачення її результатів, створення кадрового резерву – це ті завдання, які на неї покладалися завжди. Однак умови розвитку сучасної держави передбачають, що ці завдання мають бути ширшими. Так, Є. Кагановська до них відносить аналіз кадрової ситуації; прогнозування потреби в кадрах, виходячи зі стратегії розвитку державної служби; створення системи мотивації до вступу на державну службу й продуктивної діяльності у подальшому; відбір кадрів, їхнє розміщення; оцінювання кадрів, здійснення необхідних перестановок; організацію навчання державних службовців, підвищення їхньої кваліфікації; відбір і підготовку керівних

кадрів, просування по службі; виявлення соціальної напруженості та її усунення; здійснення обліку кадрів, ведення кадрової документації; контроль за дотриманням нормативних приписів, що регламентують порядок проходження служби[6, с. 279].

Реформування кадрових служб у системі державного управління вже давно на часі. Оскільки, на думку Ю. Сурміна, криза державності, що вилилась у події з 2014 р. привела до суттєвих змін у кадровій політиці. Він вживає термін «кадрова революція». У поняття вкладає швидкі зміни адміністративно-управлінських кадрів [7, с. 55].

Таким чином, вважаємо, що забезпечення кадрової безпеки є необхідною умовою реформування кадрового забезпечення у системі державного (публічного) управління в Україні. Механізми забезпечення кадрової безпеки повинні утверджуватися в контексті реформування державної служби, впровадження нових принципів державної служби в Україні, реформування кадрових служб органів державної влади та органів місцевого самоврядування. Кінцевою метою реформування має стати ефективне управління суспільними процесами.

Список використаної літератури:

1. Пархоменко-Куцевіл О. Кадрова безпека в системі державного управління України: теоретичні засади / О.Пархоменко-Куцевіл // Ефективність державного управління. – 2013. – Вип. 37. – С. 13–20.
2. Калганов Л.В. Соотношение и взаимодействие понятий государственного управления и менеджмента / Л. В. Калганов // ЮРИСТ. – 2006. – № 11. – С. 55–58.
3. Подлужна Н. О. Забезпечення кадрової безпеки організації / Н. О. Подлужна // Економіка промисловості. – 2010. – № 4. – С. 210–215.
4. Державна кадрова політика в Україні: стан, проблеми та перспективи розвитку: наукова доповідь / За загальною редакцією Ю. В. Ковбасюка, К. О. Ващенко, Ю. П. Сурміна (керівник проекту). – К.: НАДУ, 2012. – 72 с.
5. Закон України «Про державну службу» від 10 грудня 2015 р. // Відомості Верховної Ради (ВВР). – 2016. – № 4. – С. 43.

6. Кагановська Т. Є. Кадрове забезпечення державного управління в Україні: Монографія / Є. Т. Кагановська. – Х.: ХНУ імені В.Н. Каразіна, 2010. – 330 с.

7. Сурмін Ю.П. Кадрова революція в Україні: сутність, проблеми, напрями розгортання / Ю. П. Сурмін // Інституційне забезпечення кадрової політики у державному управлінні: становлення та розвиток: матеріали щоріч. Всеукр. наук.-практ. конф. за міжнар. участю (Київ, 29 трав. 2015 р.) / за заг. ред. Ю. В. Ковбасюка, А. І. Семенченка, С. В. Загороднюка. – К.: НАДУ, 2015. – С. 55-58.

Кравчук К., Заєць Т.

студентки СВО магістра

Вінницького державного педагогічного
університету імені Михайла

Коцюбинського

УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПРОЦЕСАМИ В КАРАНТИННО-ОБМЕЖУВАЛЬНИХ УМОВАХ В СИСТЕМІ СЕРЕДНЬОЇ ТА ВИЩОЇ ШКОЛИ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Управління інформаційними процесами керівника закладу освіти містить у собі обробку великих обсягів інформації. Для того щоб приймати вірні управлінські рішення, інформація повинна бути об'єктивною, надходити вчасно, відображати динаміку змін в об'єкті управління. Крім того, потрібні технології за допомогою яких керівник зможе здійснити обробку інформації швидко і точно, з мінімальними витратами часу і сил.

Сучасна освіта з кожним днем вимагає все більш активного використання інформаційно-комунікаційних технологій в управлінській, навчально-виховній, фінансовій діяльності навчального закладу особливо в карантинно-обмежувальних умовах.

Відповідно до Листа Міністерства освіти і науки №1/9-154 від 11 березня 2020 року, з 12 березня 2020 року в Україні запроваджується карантин для усіх закладів освіти. Зокрема, в листі зазначено, що учням та студентам забороняється відвідувати заклади освіти під час карантину та надано рекомендації, щодо розробки заходів для проведення занять за допомогою дистанційних технологій [1].

Зклади освіти почали працювати в карантинно-обмежувальних умовах. Одним з пріоритетних напрямів роботи загальноосвітніх і вищих шкіл визнане дистанційне навчання, яке здійснюється завдяки інформаційно-освітнім технологіям і системам комунікації.

У зв'язку із вимушеним режимом дистанційного навчання педагогічні працівники почали удосконалювати вміння працювати з цифровими інструментами й новими педагогічними підходами та методами. Це стало викликом для всіх учасників освітнього процесу.

Як визначено в наказі Міністерства освіти і науки України від 25.04.2013 № 466 “Про затвердження Положення про дистанційне навчання”, зареєстрованого в Міністерстві юстиції України 30 квітня 2013 р. за № 703/23235 [2], дистанційне навчання – це індивідуалізований процес набуття знань, умінь, навичок і способів пізнавальної діяльності людини, який відбувається в основному за опосередкованої взаємодії віддалених один від одного учасників навчального процесу у спеціалізованому середовищі, яке функціонує на базі сучасних психолого-педагогічних та інформаційно-комунікаційних технологій.

Перед керівниками закладів освіти постало завдання організувати якісне навчання з використанням цифрових технологій, адже дистанційна форма навчання передбачає доступ до інтернету, технічне забезпечення (комп’ютер, планшет, смартфон тощо) в усіх учасників освітнього процесу.

Основні форми онлайн-комунікації під час дистанційного навчання в карантинно-обмежувальний період:

Відеоконференція – це конференція в режимі реального часу онлайн. Вона проводиться у визначений день і час. Це один із сучасних способів зв’язку, що дозволяє проводити заняття коли учасники освітнього процесу перебувають на відстані. Отже, обговорення й ухвалення рішень, дискусії, захист проектів відбуваються в режимі реального часу.

Форум – найпоширеніша форма спілкування учасників освітнього процесу у дистанційному навчанні. Кожний форум присвячений певній проблемі або темі.

Чат – спілкування користувачів мережі в режимі реального часу, засіб оперативної комунікації людей через інтернет. Є кілька різновидів чатів: текстовий, голосовий, аудіо-, Основні форми онлайн-комунікації відеочат. Найбільш поширений – текстовий чат. Голосовий чат дозволяє спілкуватися за допомогою голосу, що під час вивчення іноземної мови в дистанційній формі є важливим моментом.

Блог – це форма спілкування, яка нагадує форум, де право на публікацію належить одній особі чи групі людей. Автор розміщує на сайті свого мережевого щоденника (блогу) допис (твір, есе) і на-

дає можливість іншим прочитати й прокоментувати розміщений матеріал.

Електронна пошта – це стандартний сервіс інтернету, що забезпечує передавання повідомлень як у формі звичайних текстів, так і в інших формах (графічній, звуковій, відео) у відкритому чи зашифрованому вигляді. У системі освіти електронна пошта використовується для організації спілкування.

Анкетування – для поточного контролю в ході дистанційного навчання зручно використовувати різноманітні анкети. Анкета є достатньо гнучким інструментом, оскільки питання можна ставити безліччю різних способів. У дистанційному навчанні після засвоєння кожної теми можна використовувати анкети, в учасники освітнього процесу можуть зробити самооцінку результатів навчання [3].

Соціальні мережі, служби обміну миттєвими повідомленнями та мобільні застосунки типу Viber дозволяють створювати закриті групи, спільноти, чати, вести обговорення тем, завдань, проблем, інформації.

На сучасному етапі основними інструментами для організації дистанційного навчання в карантинно-обмежувальний період слугують Веб-ресурси:

Платформа Moodle – безкоштовна відкрита система управління дистанційним навчанням. Дозволяє використовувати широкий набір інструментів для освітньої взаємодії учасників освітнього процесу та адміністрації закладу освіти.

Платформа Google Classroom – це сервіс, що пов'язує Google Docs, Google Drive і Gmail, дозволяє організувати онлайн-навчання, використовуючи відео-, текстову та графічну інформацію.

Zoom – сервіс для проведення відеоконференцій та онлайн-зустрічей. Для цього потрібно створити обліковий запис. Безкоштовна версія програми дозволяє проводити відеоконференцію тривалістю 40 хвилин, однак на період пандемії сервіс зняв це обмеження. Zoom підходить для індивідуальних та групових занять. Користувачі можуть використовувати додаток як на комп'ютері, так і на планшеті чи смартфоні.

Відеоконференції можна проводити також за допомогою Microsoft Teams, Google Meet, Skype тощо

ClassDojo – простий інструмент для оцінювання роботи класу в режимі реального часу. Тут створена комфортна система заохочення з різними ролями та рівнями доступу. Кожен учасник освітнього процесу отримує аватарку у вигляді монстрика. Завдання монстрика – збирати бали за завдання. За кожне завдання викладач присвоює учням певну кількість балів.

Classtime – платформа для створення інтерактивних навчальних додатків, яка дозволяє вести аналітику навчального процесу і реалізовувати стратегії індивідуального підходу. Є бібліотека ресурсів, а також можливість створювати запитання.

LearningApps.org – онлайн-сервіс, який дозволяє створювати інтерактивні вправи. Їх можна використовувати в роботі з інтерактивною дошкою або як індивідуальні вправи для учасників навчального процесу. Тут можна створювати вправи для використання з інтерактивною дошкою [3].

Одним із недоліків дистанційного навчання в Україні є відсутність або низька якість Інтернету в окремих населених пунктах.

Саме тому, завдяки спільним зусиллям Офісу Президента України, Міністерства освіти і науки України, Комітету Верховної Ради України з питань освіти, науки та інновацій, Дитячого фонду ООН (ЮНІСЕФ), Pinchuk Art Centre, Національного художнього музею України, проекту “Книга-мандрівка. Україна”, громадської спільки “Освіторія”, а також понад 20-ом педагогам, 6 квітня 2020 року для учнів 5-11 класів з усієї країни стартував проект «Всеукраїнська школа онлайн». Основна мета проекту – створити для кожного українського учня, незалежно від місця проживання, ресурсів та можливості підтримати зв'язок зі своїми вчителями, доступ до знань.

В рамках проекту передбачено уроки з 11 предметів: української мови, української літератури, історії України, всесвітньої історії, англійської мови, фізики, алгебри, геометрії, географії, хімії, біології. Уроки чітким розкладом транслюють українські телеканали та YouTube канал Міністерства освіти і науки.

28 квітня 2020 року в межах проекту розпочались також трансляції для учнів 1-4 класів. Програма початкової школи розрахована на 5 тижнів і складається з чотирьох предметів: української мови, математики, науки та мистецтва.

Зйомки уроків відбуваються у Новопечерській школі м. Києва. У відеозаняттях взяли участь українські зірки: ведучі, музиканти, актори, спортсмени тощо. Вони відповідають на запитання, вирішують задачі та проводять досліди разом з учителями [4].

Дистанційна форма навчання має ряд беззаперечних переваг. Зокрема, у закладах вищої освіти здобувач освіти може навчатися у зручний для нього час, звичному оточенні та у відносно автономному темпі. Проте, система дистанційного навчання має і недоліки. По-перше, для успішної корекції навчання та адекватного оцінювання важливо мати безпосередній контакт із здобувачем. Крім того, неможливо точно перевірити, чи саме та людина працює, виконує завдання чи це робить хтось інший. Тому в минулі роки остаточний контроль якості знань все ж таки проводився на очній сесії.

На даний час, в умовах карантину та дистанційного навчання Міністерство освіти і науки розробило і надіслало керівникам закладів освіти Лист «Щодо організації поточного, семестрового контролю та атестації здобувачів освіти із застосуванням дистанційних технологій навчання» і «Рекомендації щодо організації поточного, семестрового контролю та атестації здобувачів фахової передвищої та вищої освіти із застосуванням дистанційних технологій навчання» [5].

В рекомендаціях Міністерства освіти і науки зазначено, дистанційна комунікація учасників освітнього процесу може здійснюватися через засоби комунікації, вбудовані до системи управління навчанням (LMS), електронну пошту, месенджери (Viber, Telegram та ін.), відеоконференції (MS Teams, ZOOM, Google Meet, Skype та ін.), форуми, чати тощо. Рекомендовано використання закладом освіти єдиної LMS та єдиного інструменту комунікацій, закріпленого нормативними документами закладу.

Також МОН рекомендує закладам використовувати єдиний інструмент комунікацій під час проведення оцінювання та атестації студентів та закріпити його у власних нормативних документах. А вченим радам варто внести зміни та доповнення до Положень про організацію освітнього процесу та Положень про екзаменаційну комісію та передбачити в цих документах застосування запропонованих заходів для дистанційного проведення оцінювання.

Міністерство звертає увагу закладів освіти на важливість забезпечення належного контролю, зокрема використання авторизованого доступу до комунікаційних інструментів, фіксацію часу початку та завершення виконання студентом завдання, використання алгоритмів випадкового вибору завдань тощо.

МОН надало алгоритми проведення поточного та семестрового контролю, а також атестації та її документального супроводу. Міністерство пропонує закладам проводити захисти кваліфікаційних робіт із використанням відеозв'язку. А паперовий примірник кваліфікаційної роботи з власноручним підписом здобувача може бути надісланий поштою заздалегідь до екзаменаційної комісії, або ж, за умови використання в закладі електронного документообігу, електронний примірник, засвідчений кваліфікованим електронним цифровим підписом. Рекомендації МОН водночас є переліком пропозицій, що не обмежують заклади освіти в межах їхньої академічної автономії у пошуку та реалізації інших слушних рішень із організації дистанційного навчання [5].

В умовах дистанційного навчання в середній школі, коли значну частину матеріалу учні засвоїли самостійно, особливої ваги набуває формувальне оцінювання. Важливо якомога частіше давати учням зворотний зв'язок: відзначати успіхи, щоб зберігати мотивацію, надавати поради про те, що потребує додаткового опрацювання, хвалити за помилки, якщо вони виявлені самим учнем.

Оцінювання відбуватиметься в режимі онлайн – якщо є технічна можливість, то на дистанційних платформах, на яких існує така функція. Працюючи на платформах, учні можуть посперечатися з однокласниками, обговорити проблеми, висловити власну думку, побачити і почути їхню думку про свої досягнення (взаємооцінювання). Учитель може запропонувати учням поміркувати про власне оцінювання, попросити учнів оцінити свої знання з теми, порівняти з тим, що вони знали, і визначити, що нове дізнались (самооцінювання).

Отримання навчальних матеріалів та спілкування між учасниками дистанційного навчання під час оцінювання, що проводиться дистанційно, забезпечується передачею відео, аудіо, графічної та текстової інформації в синхронному або асинхронному режимі. Це

можуть бути письмові роботи (самостійні й контрольні, перекази, у тому числі окремі тестові завдання тощо), а також навчальний проект, заповнення таблиць, побудова схем, моделей тощо.

У разі потреби завдання учнів можна контролювати через будь-який месенджер, що забезпечує відозв'язок (Zoom, Skype тощо). Оскільки на сьогодні не розроблено єдину систему оцінювання для дистанційної форми навчання, учасники освітнього процесу за домовленістю можуть користуватися тими засобами, які комфортні для всіх [3].

Отже, використання інформаційних процесів для управління закладами освіти є необхідним на сучасному етапі не тільки під час карантинно-обмежувальних умов. Цю необхідність диктують, перш за все, високі вимоги, що пред'являються до рівня кваліфікації працівників на всіх рівнях управління. Присутність сучасних технологій в освітньому процесі надає можливість не тільки отримання інформації, її застосування, а й можливість дистанційного навчання у сфері освіти. Інформаційні процеси в управлінні закладами освіти сприяють підвищенню якості освітнього процесу, так як розвиток навчального процесу в сучасних умовах розглядається як процес змін, підвищення якості освіти.

Список використаної літератури:

1. Лист МОН №1/9-154 від 11 березня 2020 р. щодо запровадження карантину // Міністерства освіти і науки України. – Режим доступу: https://mon.gov.ua/storage/app/media/news/%D0%9D%D0%BE%D0%B2%D0%B8%D0%BD%D0%B8/2020/03/11/1_9-154.pdf.
2. Положення про дистанційне навчання // Міністерство освіти і науки України. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/z0703-13>.
3. Коберник І. Організація дистанційного навчання в школі. Методичні рекомендації / І. Коберник, З. Звиняцьківська., 2020. – 71 с.
4. Всеукраїнська школа онлайн // Міністерство освіти і науки. – Режим доступу: <https://mon.gov.ua/ua/tag/vseukrayinska-shkola-onlajn>
5. Рекомендації щодо організації поточного, семестрового контролю та атестації здобувачів фахової передвищої та вищої освіти

ти із застосуванням дистанційних технологій навчання // Міністерство освіти і науки України. – Режим доступу: <https://mon.gov.ua/ua/npa/shodo-organizaciyi-potochnogo-semestrovogo-kontrolyu-ta-atestaciyi-zdobuvachiv-osviti-iz-zastosuvannyam-distancijnih-tehnologij>.

6. Як дистанційно проводити сесію та атестацію студентів: МОН надіслало університетам і коледжам методичні рекомендації // Міністерство освіти і науки. – Режим доступу: <https://mon.gov.ua/ua/news/yak-distancijno-provoditi-sesiyu-ta-atestaciyu-studentiv-mon-nadislalo-universitetam-i-koledzham-metodichni-rekomendaciyi>

Мар'яш В.Ю.

магістр

«ПОСАДИ В СИСТЕМІ ДЕРЖАВНОГО УПРАВЛІННЯ УКРАЇНИ. ПРОБЛЕМНІ ПИТАННЯ КЛАСИФІКАЦІЇ ПОСАД»

Державне управління (публічне управління, англ. Public administration) – вид діяльності держави, здійснення управлінського організуючого впливу шляхом використання повноважень виконавчої влади через організацію виконання законів, здійснення управлінських функцій з метою комплексного соціально-економічного та культурного розвитку держави, її окремих територій, а також забезпечення реалізації державної політики у відповідних сферах суспільного життя, створення умов для реалізації громадянами їх прав і свобод.

Державне управління є складовою політичного управління, тобто є процесом реалізації державної виконавчої влади як засобу функціонування будь-якої соціальної спільноти.

Вид та обсяг правової відповідальності є необхідною і достатньою умовою для визначення виду робіт, а відтак і посад, які підпадають під дію законодавства з питань публічної служби, а відповідні громадяни мають статус публічних службовців. У такому сенсі правова відповідальність, що включає зміст, характер роботи та контроль за її виконанням і санкції, є критерієм класифікації посад публічних службовців.

Феноменом поняття “публічна служба”, попри різні доктринальні та нормативні визначення, є не стільки процес або результат виконання певних публічно-владних функцій чи “роботи” в суспільних інтересах загалом і насамперед в інтересах громадянина, громади та народу, а необхідна та достатня умова задоволення суспільного інтересу, очікування, запиту;

Для сучасної України багато викликів державотворення були надзвичайно складними через тягар радянського минулого та відсутність достатніх знань у сфері демократичного урядування. До нерозроблених, а також досліджуваних у певних ідеологічних рамках, питань, на лежав і інститут публічної служби. Можна конста-

тувати, що і дотепер для українського адміністративного права навіть саме поняття «публічної служби» є новим.

До публічних політичних посад варто віднести наступні посади: Президента України; Главу Адміністрації Президента України та його заступників Постійного Представника Президента України в Автономній Республіці Крим та його заступників; членів Кабінету Міністрів України, перших заступників та заступників міністрів; постійного представника Кабінету Міністрів України у Конституційному Суді України; народних депутатів України; Уповноваженого Верховної Ради України з прав людини та його представників; голів місцевих державних адміністрацій, їх перших заступників та заступників.

Принцип підпорядкованості, ієрархії. Кожна складова системи публічної служби займає своє місце у структурі системи публічної служби, а також принцип підпорядкованості передбачає наявність власної структури з внутрішніми взаємозв'язками структурних елементів. За даним принципом слід проаналізувати горизонтальні, вертикальні та інші види зв'язків між елементами системи.

Принцип безперервної діяльності. Сервісний характер публічної служби передбачає постійне надання послуг громадянам. Тому статус служби, яка набуває статусу публічної, має передбачати виконання публічних функцій на постійній основі, а також має бути законодавчо передбачений механізм постійного виконання публічних функцій у випадках зміни статусу, відмови, припинення надання публічних послуг певною службою.

Якщо розглядати державну владу та місцеву самоврядну владу як складові публічної служби, то слід розглядати також і функції державної та самоврядної влади як складові функцій публічної служби. Отже, функціями органів державної влади виступають основні напрями їх діяльності, в яких виявляється їх сутність і призначення в державному механізмі. Кожна інституція відповідно до своєї компетенції виконує притаманні йому функції. У зв'язку ще з невизначеним понятійним навантаженням системи публічної служби у вітчизняній науці використовуємо поняття "суб'єкта публічної служби" як будь-якої публічної інституції, що здійснює функції публічної служби. Основна ознака функцій публічної служби – задоволення публічного інтересу шляхом надавання

публічних послуг; виконання функцій публічної влади; виконання функцій та завдань публічних інституцій.

Варто зазначити, що чинне законодавство України закріпило поняття «посада державної служби», яке необхідно відмежовувати з поняттям «державна посада», яке використовується у законодавстві деяких зарубіжних країн (починаючи від Стародавнього Риму, до сучасних Угорщини, Болгарії, Греції), проте у законодавстві України не використовується, хоча у літературі зустрічається аналіз саме «державних посад» як об'єктів державного управління. Ці поняття не слід ототожнювати, оскільки не кожна посада у державному органі може бути посадою професійної публічної служби.

Органи, які здійснюють державне управління, – це виконавчі структури, що й відображено в їх назві (органи виконавчої влади). Основним їх призначенням є організація виконання законодавчих актів, прийнятих парламентом, та актів глави держави.

Масштабність державного управління означає, що ця державно-управлінська діяльність є найоб'ємнішою в державі. Вона розповсюджується на всю її територію та величезну кількість об'єктів управління. До сфери його безпосереднього відання належать правові, інформаційні, економічні, фінансові, технічні, організаційні, людські та інші ресурси, що є в наявності у держави.

Універсальність державного управління виражається через діяльність органів виконавчої влади, яка є безперервною, тобто вона неможлива без повсякденного і постійного управлінського впливу на суспільні відносини, охоплюючи всі, без винятку, сфери суспільного життя та здійснюється на всіх рівнях управління – від центру до регіонів та конкретних територій.

Класифікуючи посади системи державної цивільної служби як підсистеми державного (публічного) управління, слід виокремлювати посади:

- політичних службовців (на відміну від посад політичних діячів) – це посади, які зазнають політичного впливу- безпосереднього впливу політичних діячів;
- адміністративні (службові). У процесі класифікації посад системи місцевого самоврядування як підсистеми державного (публічного) управління слід виокремлювати посади:

- представницькі – виборні посади (на які обирають територіальною громадою або відповідною радою);
- адміністративні (службові).

Надзвичайно важливе значення для розуміння сутності інституту публічної служби мають принципи публічної служби. У суспільних науках під принципами зазвичай розуміють вихідні положення і теоретичні ідеї, які відображають об'єктивні закономірності розвитку суспільства і держави. Принципи публічної служби – це основоположні ідеї, які відбивають об'єктивні закономірності та визначають напрямки реалізації компетенції, завдань і функцій органів публічної влади, статусу публічних службовців. Вони зумовлюють значимість, закономірність і соціальну цінність відносин, які виникають у системі публічної служби. При цьому всі принципи взаємопов'язані: дотримання одних сприяє реалізації інших, і навпаки, порушення будь-якого з принципів негативно впливає на виконання інших принципів. Основною метою правового закріплення принципів публічної служби є визначення засад організації і функціонування публічної служби.

1) кар'єрний публічний службовець – це публічний службовець, який прийнятий на посаду на невизначений термін та має можливість реалізувати своє право на кар'єрне зростання згідно процедури, визначеної законом;

2) публічний службовець політичної (особистої) відданості – це публічний службовець, прийнятий на посаду на термін повноважень державного політика або колегіальної державної інституції, що найняла його;

3) публічний керівник – це публічний службовець, якого прийнято на конкурсній основі або на основі політичної (особистої) вірності главі держави або муніципальній інституції або агенції;

4) тимчасово виконуючий обов'язки публічний службовець – це публічний службовець, що заміняє кар'єрного публічного службовця, що тимчасово не може виконувати свої обов'язки.

В цьому випадку були одночасно застосовані такі критерії для класифікації, як політичність та строковість призначення. Хоча, не найкращим, на наш погляд, є віднесення взагалі до посад публічної служби політичних посад, оскільки це розмиває межі публічної служби.

Тишківська А.В.

здобувач СВО магістра факультету
історії, права і публічного управління
ВДПУ ім. М. Коцюбинського

ВИКОРИСТАННЯ ЗАКЛАДАМИ ВИЩОЇ ОСВІТИ ЄДЕБО В КОНТЕКСТІ БЕЗПЕКИ ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ (НА ПРИКЛАДІ ВДПУ)

За умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій (далі – ІКТ) у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки. Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому унеможлиблюється нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

На основі положень і нормативно-правових актів, за якими функціонує ВДПУ ім.М.Коцюбинського, можна виокремити принцип інформаційної безпеки в освітньому процесі [4, с.175].

Принцип інформаційної безпеки забезпечує на кожному етапі впровадження освітньої інформації, спеціальну систему дій, що перешкоджають несанкціонованому доступу до інформації, порушенню цілісності, поширенню конфіденційної й персональної інформації про суб'єкти інноваційного процесу; передбачає визначення інформації закритого типу й інструкції щодо доступу до неї користувачів, а також забезпечення захисту авторських прав об'єктів інтелектуальної власності. Особливе значення має проблема розміщення й захисту інформації в мережі Інтернет, що посилюється низьким рівнем інформаційної культури користувачів. Ці дії спрямовані на оптимальне співвідношення між доступом і захистом інформації, інформаційних ресурсів і продуктів інноваційної діяльності у системі інформаційного забезпечення.

Інформаційно-комунікаційне забезпечення ВДПУ ім.М.Коцюбинського здійснюється за допомогою Єдиної державної електронної бази з питань освіти (далі – ЄДЕБО) та офіційного сайту навчального закладу [1, 2].

ЄДЕБО є автоматизованою системою збирання, реєстрації, обробки, зберігання та захисту відомостей та даних з питань освіти, що передбачені законом, актами Кабінету Міністрів України та іншими нормативно-правовими актами [5,6].

Головним призначенням ЄДЕБО є забезпечення органів державної влади, органів місцевого самоврядування, фізичних та юридичних осіб інформацією в галузі освіти щодо навчальних закладів, документів про освіту та наукові ступені, результатів зовнішнього незалежного оцінювання, перебігу вступної кампанії до навчальних закладів, студентських квитків державного зразка, іншою інформацією в галузі освіти.

Завдяки використанню ЄДЕБО забезпечується робота таких сервісів ВДПУ ім.М.Коцюбинського:

- автоматизація ліцензування освітньої діяльності у сфері вищої та післядипломної освіти;
- забезпечення вступу до ВДПУ ім.М.Коцюбинського шляхом подання документів через Інтернет (електронний вступ);
- формування рейтингових списків вступників та списків вступників, рекомендованих до зарахування до ВДПУ ім.М.Коцюбинського;
- забезпечення автоматизованого розподілу місць державного замовлення;
- інформування громадськості про перебіг вступної кампанії до ВДПУ ім.М.Коцюбинського;
- формування, реєстрація та облік відомостей та даних, що відтворюються в документах ВДПУ ім.М.Коцюбинського;
- перевірка достовірності документів про освіту та наукові ступені, студентських квитків державного зразка, ліцензій на провадження освітньої діяльності, сертифікатів про акредитацію та свідоцтв про атестацію;
- формування статистичних звітів [6].

Важливе значення у функціонуванні ЄДЕБО має дотримання вимог законодавства про захист персональних даних. Тому у ВДПУ

ім. М. Коцюбинського відомості та дані вносяться до ЄДЕБО за допомогою спеціалізованого програмного забезпечення особами, які уповноважені ректором ВДПУ ім.М.Коцюбинського (технічні секретарі) [3].

До реєстру навчальних закладів внесено відомості про ВДПУ ім.М.Коцюбинського, її структурні підрозділи:

- повне найменування (та скорочене у разі його наявності);
- ідентифікаційний код;
- найменування органу, до сфери управління якого належить;
- місцезнаходження;
- прізвище, ім'я, по батькові, посада, освіта, наукові ступені і вчені звання, номер телефону та адреса електронної пошти керівника навчального закладу/наукової установи та керівників підрозділів;
- відомості про матеріально-технічне забезпечення освітньої діяльності;
- відомості про ліцензії на провадження освітньої діяльності, в тому числі ті, що анульовані чи втратили чинність, а також відомості, на підставі яких видавалися ліцензії на провадження освітньої діяльності;
- відомості про акредитацію, атестацію навчального закладу/наукової установи, в тому числі ті, що втратили чинність, відомості, на підставі яких приймалися рішення про акредитацію чи атестацію;
- відомості про кількість здобувачів освіти за спеціальностями, професіями, рівнями освіти, роками навчання, за окремими категоріями, визначеними розпорядником Єдиної бази;
- відомості про кількість наукових, науково-педагогічних та педагогічних працівників за посадами, освітою, науковими ступенями і вченими званнями;
- відомості про результати перевірок дотримання навчальними закладами/науковими установами ліцензійних умов, аудиторських перевірок, інспектування навчального закладу/наукової установи;
- звіти навчального закладу/наукової установи, в тому числі фінансові, передбачені законодавством.

В процесі публічно-управлінської діяльності (при прийомі на роботу, переведенні на посади, прийнятті рішення про надбавки

до заробітної платні, вступі та поновленні здобувачів вищої освіти та ін.) використовується реєстр документів про освіту ЄДЕБО, який містить відомості про документи про освіту та наукові ступені, створені відповідно до законодавства. Зокрема, відомості про:

- документи про освіту та наукові ступені державного зразка, видані навчальними закладами/науковими установами України з 2000 року;

- власні документи про вищу освіту, видані ВДПУ ім.М.Коцюбинського;

- спільні та подвійні дипломи, видані вищими навчальними закладами України;

- документи про вищу освіту, видані іноземними навчальними закладами, із свідоцтвами про їх державне визнання, виданими МОН;

- документи про вищу духовну освіту із свідоцтвами про їх державне визнання, виданими МОН;

- документи про вищу освіту, видані іноземними навчальними закладами, з рішеннями вищого навчального закладу України про їх визнання [5].

Враховуючи, що основним завданням ВДПУ ім.М.Коцюбинського є підготовка здобувачів вищої освіти, активно ЄДЕБО використовується під час вступної кампанії. Зокрема, реєстр сертифікатів зовнішнього незалежного оцінювання надає дані, внесені в Єдину базу Українським центром оцінювання якості освіти. На основі реєстру сертифікатів зовнішнього незалежного оцінювання ВДПУ ім.М.Коцюбинського отримує можливість електронного вступу та розподілу державного замовлення на підготовку здобувачів вищої освіти.

Реєстр студентських квитків державного зразка забезпечує облік студентських квитків ВДПУ ім.М.Коцюбинського, можливість перевірки їх достовірності, а також підтвердження факту навчання студентів та їх права на отримання соціальної допомоги та пільг.

Отже, проблема інформаційної безпеки є одним з найважливіших напрямів, що потребує вдосконалення на рівні публічного адміністрування. А використання ЄДЕБО є, безумовно, прогресивним рішенням за умови виконання вимог із захисту інформації.

Список використаної літератури:

1. Деякі питання реалізації у 2015–2017 рр. Державної стратегії регіонального розвитку на період до 2020 р. : Постанова Кабінету Міністрів України від 7 жовтня 2015 р. № 821. – Режим доступу : <http://zakon1.rada.gov.ua/laws/show/821-2015-%D0%BF>.
2. Деякі питання створення Єдиної бази : Наказ Міністерства освіти і науки України від 31.12.2010 № 1341// Вища освіта – 2011. – Режим доступу: http://osvita.ua/legislation/Vishya_osvita/18237/ (дата доступу:14.10.2015).
3. Джафарова О.В. Дослідження органів публічної адміністрації в системі суб'єктів дозвільної діяльності в Україні / О.Джафаров // Форум права – 2016 – №1 – С.42-49.
4. Патерило І.В. Інструменти діяльності публічної адміністрації: сутність та зміст /І.В.Патерило //Науковий вісник Ужгородського національного університету. Серія «Право». – 2014. – Вип. 27. – Т. 2. – С. 174–178.
5. Про внесення зміни до пункту 3 Положення про Єдину державну електронну базу з питань освіти: Постанова Кабінету Міністрів України від 27 серп. 2014 р. № 391 // Верховна Рада України. – Режим доступу: <http://zakon4.rada.gov.ua/laws/show/391-2014-п>.
6. Про створення Єдиної державної електронної бази з питань освіти : Постанова Кабінету Міністрів України від 13 лип. 2011 р. № 752 // Верховна Рада України. Режим доступу: <http://zakon4.rada.gov.ua/laws/show/752-2011-п>.

Франко Л.І., Франко І.О.

здобувачі СВО магістра,
Вінницький державний
педагогічний університет
імені М. Коцюбинського

ПУБЛІЧНЕ АДМІНІСТРУВАННЯ ЗАКЛАДІВ ОХОРОНИ ЗДОРОВ'Я В УМОВАХ КАРАНТИНУ

В умовах загальносвітового карантину, викликаного пандемією корона вірусу, публічне адміністрування закладів охорони здоров'я (далі – ЗОЗ) є необхідною умовою для їх забезпечення та належного функціонування. Основним завданням ЗОЗ є забезпечення надання якісної і своєчасної висококваліфікованої медичної допомоги населенню.

Зауважимо, що в умовах реформування медичної галузі в Україні (а реформа даної сфери - це тривалий процес, який розпочався з 2018 року) карантин допоміг переосмислити певні підходи до адміністрування ЗОЗ.

В сучасних умовах з березня 2020 р. адміністрація всіх медичних закладів України переведена в режим підвищеної готовності, керівники зобов'язані перебувати цілодобово на зв'язку. Крім того, найближчим часом жоден не може взяти відпустку. Директори інфекційних лікарень мають подати інформацію про медичне обладнання, яке необхідно закупити для лікування пацієнтів з коронавірусом. У випадку лікування вагітних, породіль та новонароджених, уражених коронавірусом, мають розробити алгоритм дій. Провести інвентаризацію апаратів штучної вентиляції легень у підпорядкованих медичних закладах. Приватним ЗОЗ, в тому числі стоматологічним поліклінікам, наказано розробити алгоритм дій в умовах карантину та розглянути питання виділення коштів з резервного фонду для закупівлі засобів індивідуального захисту [1,с.3-5].

Накази міністерства охорони здоров'я передбачали організаційні зміни у ЗОЗ, зокрема, визначено заклади, які можуть найкраще реорганізуватися аби прийняти велику кількість пацієнтів, розроблено та затверджено низку документів абсолютно нових по змісту

нормативних актів, які визначають функціонування ЗОЗ в Україні. Докладніше проаналізуємо їх зміст.

Наразі основним документом в умовах пандемії коронавірусу є наказ Міністерства охорони здоров'я (далі - МОЗ) від 13.03.2020 №663 «Про оптимізацію заходів щодо недопущення занесення і поширення на території України випадків COVID-19» [2,с.3,4]. Зауважимо, що для керівників медичних закладів цей наказ став настільною книгою, оскільки саме вони несуть персональну відповідальність за виконання комплексу заходів, передбачених цим документом.

МОЗ України чітко повідомило, що всі медичні послуги, ненадання яких несе серйозний ризик для життя пацієнта або може призвести до ризику розвитку критичних станів, будуть надаватися в повному обсязі і вчасно. До них віднесені наступні категорії:

- вагітні, породіллі і новонароджені;
- випадки ускладненого перебігу вагітності і пологів;
- спеціалізовані відділення медзакладів для онкохворих;
- захворювання, які потребують кардіоторакальних оперативних втручань у разі, коли припинення (відтермінування) такої медичної допомоги має серйозний ризик для життя і здоров'я [1,с.3].

Крім цього, ніяких змін не відбудеться в наданні паліативної медичної допомоги у стаціонарних умовах, а також при інших невідкладних і термінових госпіталізація та планових операціях, коли відтермінування надання меддопомоги несе серйозний ризик для життя і розвитку життєзагрожуючих станів.

Своєю чергою, МОЗ України направило в регіони рекомендації щодо відтермінування планових операції та надання інших медичних послуг для запобігання поширенню на території України корона вірусу COVID-19 .[4.с.5]

Як показав досвід інших держав, зокрема, Італії медичні системи охорони здоров'я не дають собі рад з великою кількістю захворілих. Оперативні заходи (карантинні), які прийняті в Україні, дозволили зменшити епідемію, принаймні, до тих пір, аби заклади могли впоратися з зростанням кількості пацієнтів.

Таким чином, основним завдання в управлінні ЗОЗ України є забезпечення якісної і своєчасної медичної допомоги суспільству

та забезпечення прав і свобод громадян на території України. Особлива увага повинна приділятися своєчасному повному забезпеченню закладів ліками та засобами медичного призначення, від яких залежить рівень надання медичної допомоги.

Список використаної літератури

1. Наказ Міністерства охорони здоров'я України №663 « Про оптимізацію заходів щодо недопущення занесення і поширення на території України випадків COVID-19» від 13.03.2020р.[Електронний ресурс] Режимдоступу:<http://chnpu.edu.ua/news/important-information/item/2636-nakaz-pro-zaprovalzhennia-karantynu>.

2.Наказ №158 від 23.04.2020 року Про додаткові заходи щодо запобігання розповсюдженню коронавірусу COVID-19 [Електронний ресурс] Режим доступу :<http://chnpu.edu.ua/news/important-information/item/2636-nakaz-pro-zaprovalzhennia-karantynu>

3 Наказ №150 від 27.03.2020 року Про додаткові заходи щодо запобігання розповсюдженню коронавірусу COVID-19.[Електроннийресурс]Режимдоступу <http://chnpu.edu.ua/news/important-information/item/2636-nakaz-pro-zaprovalzhennia-karantynu>

4.Наказ №148 від 17.03.2020 року Про організаційні заходи длязапобігання поширенню коронавірусу COVID-19.[Електронний ресурс] Режим доступу <http://chnpu.edu.ua/news/important-information/item/2636-nakaz-pro-zaprovalzhennia-karantynu>

5. Наказ №147 від 11.03.2020 року Про запровадження карантину з метою запобігання поширенню коронавірусу COVID-19. [Електронний ресурс] Режим доступу <http://chnpu.edu.ua/news/important-information/item/2636-nakaz-pro-zaprovalzhennia-karantynu>

Черненко Д.С.

здобувач СВО магістра,
Вінницький державний педагогічний
університет ім. М.Коцюбинського
Науковий керівник – Лазор Олег
Ярославович – доктор наук з дер-
жавного управління, професор,
професор кафедри правових наук та
філософії Вінницького державного
педагогічного університету.

ЦИФРОВА ГРАМОТНІСТЬ ЯК ЕЛЕМЕНТ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЛЮДИНИ

Цифровізація економіки призводить до проникнення технологій в особистий простір кожної людини. Широке поширення цифрових технологій в повсякденному житті впливає на взаємодію з середовищем – змінюються способи доступу до різноманітних послуг, інформації, знань, і ця взаємодія здійснюється через різноманітні канали: соціальні мережі, користування онлайн-сервісами, використання інструментів електронної демократії, покупки в інтернеті, перегляд відеоконтенту, допомога чат-ботів тощо, причому асортимент цих каналів постійно розширюється.

За даними дослідження Дослідницького холдингу Factum Group Ukraine, проведеного на замовлення Інтернет-асоціації України, наприкінці 2019 року інтернет регулярно використовували 71% (22,96 млн) населення України. Спостерігається інтенсивна динаміка охоплення нової аудиторії – ще в першому кварталі 2019 року інтернетом користувались 64% українців. Технології стають все більш доступними та дружніми до людей, зростає кількість володарів смартфонів – станом на кінець 2019 року для виходу у всевітню мережу смартфон використовували 66% інтернет-користувачів (61% на початку 2019 року). За віком розподіл користувачів виглядає наступним чином: підлітки та молодь віком від 15 до 24 років складають 15%, найбільша кількість інтернет-користувачів серед осіб віком 25-34 років (25%) та 35-44 років – 21%, особи віком

від 45 до 54 складають 18% від загальної кількості користувачів, найменші категорії: особи віком від 55 до 64 років – 12% та старші 65 років – 8% [1].

Однак темпи цифровізації перевищують розвиток навичок і умінь в області застосування засобів цифрового середовища більшості людей. Незважаючи на всі переваги, які надає інтернет, він може бути використаний для нанесення шкоди людям та їхньому майну. Різного роду шахраї, переслідувачі, різноманітні віруси – все це становить загрозу для кожного користувача мережі Інтернет. Більш того, кількість подібних загроз постійно зростає, й найбільш вразливою групою є недосвідчені користувачі. Саме тому гостро постає питання про цифрову грамотність населення.

Цифрова грамотність визначається набором знань і розумінь, які необхідні для безпечного і ефективного використання цифрових технологій та ресурсів інтернету. В основі цифрової грамотності лежать відповідні цифрові компетенції та цифрові навички.

Користувачькі цифрові навички можна умовно поділити на базові і похідні. Базові цифрові навички пов'язані з функціональною грамотністю у використанні електронних пристроїв і додатків. Вони необхідні для отримання доступу і використання цифрових пристроїв і онлайн-сервісів, тобто критично важливі для кожної людини. До них можна віднести вміння працювати з різними технічними пристроями, файлами, інтернетом, онлайн-сервісами, додатками. Сюди ж можна включити психомоторні навички, наприклад, вміння друкувати на клавіатурі або роботу з сенсорними екранами. Похідні цифрові навички пов'язані з умінням свідомо застосовувати цифрові технології в релевантному контексті в побуті і на робочому місці. Оволодіння такими навичками націлене на ефективне і осмислене використання цифрових технологій і отримання практичних результатів. Тут важливі творчі навички для роботи в онлайн-додатках і цифрових сервісах (соціальних мережах, месенджерах, інформаційних порталах), здатність створювати цифровий контент і в цілому вміння працювати з інформацією – збирати, структурувати, перевіряти на достовірність, зберігати і захищати дані [2].

У запропонованому відповідно до звіту Європейського союзу «Модель цифрових компетенцій для громадян (The Digital

Competence Framework for Citizens)» переліку цифрових компетенцій окремо представлена область «Безпека». В даній області, зокрема, виділені наступні компетенції, якими повинна володіти сучасна людина, та рекомендації до них:

1) Захист пристрою

Рекомендовано вміти забезпечувати захист пристроїв і цифрового контенту. розуміти ризики і загрози в цифровому середовищі. Знати про заходи забезпечення безпеки даних.

2) Захист персональних даних і забезпечення конфіденційності

Рекомендовано знати, як забезпечувати захист персональних даних і конфіденційність в цифровому середовищі. Розуміти, як користуватися персональною інформацією для запобігання шкоди.

3) Захист здоров'я і благополуччя

Необхідно знати, як уникати ризиків для здоров'я і загроз фізичному і психологічному здоров'ю в процесі використання цифрових технологій. Вміти захистити себе і інших від можливих небезпек в цифровому середовищі. Бути обізнаним щодо цифрових технологій для соціального благополуччя і інтеграції[3].

Отже, подолати інформаційну небезпеку можливо лише у випадку здатності людини правильно оцінювати ступінь загроз та вміння перешкоджати їм. Набута цифрова грамотність дозволить користувачу розвинути критичний аналіз змісту інформації, відповідально, усвідомлено і безпечно використовувати інструменти доступу до даних чи онлайн-послуг, застосовувати належний рівень захисту своїх пристроїв. Тому, щоб почуватися інформаційно захищеним, кожному недосвідченому користувачеві потрібно навчитися забезпечувати безпеку своїх персональних комп'ютерів та мобільних пристроїв за допомогою застосування антивірусних програм, фільтрів тощо, вміти уникати шкідливих завантажень та фішингу, надавати перевагу ліцензійному або перевіреному програмному забезпеченню, ввести практику резервного копіювання. Вкрай необхідно оволодіти базовими навиками безпечної роботи у мережі, навчитися здійснювати грамотні налаштування приватності, встановлювати надійні паролі та періодично змінювати їх, розуміти важливість зберігання конфіденційної інформації (адреси, паролі, дані рахунків, особисті відомості тощо). Безпека людини

залежить і від вміння оцінювати достовірність джерел інформації в інтернеті, виявляти пильність до методів кібершахраїв, відповідально ставитися до правил здійснення онлайн-покупок. Корисним буде навчитися керувати своєю цифровою ідентичністю та вміти захистити свою репутацію в мережі.

Однак перелік наведених навиків не є достатнім та незмінним. Ми вступаємо в епоху всебічної цифрової трансформації, яка охоплює всі галузі економіки і змінює підходи до життя і роботи. Людство буде завантажено в дані, глобально пов'язано за допомогою мобільних технологічних середовищ, розумних будинків і міст, безпілотних літальних апаратів, вуличної робототехніки [2]. Все активніше розвиватимуться такі технологічні тренди, як мобільний інтернет, інтернет речей, штучний інтелект, великі дані, VR/AR-технології (віртуальна і доповнена реальності), та багато інших, що крім переваг принесуть і додаткову небезпеку, яку потрібно враховувати та якій слід вміти протидіяти.

Наприклад, багато пасток містить некомпетентне користування мобільним інтернетом. Користувачеві потрібно усвідомлювати, що мобільні оператори, браузері, соціальні мережі можуть збирати інформацію про поточне місце розташування мобільного пристрою, характеристики найближчих точок доступу до мережі, всі дії, здійснювані на смартфоні, зчитувати інформацію про пристрій тощо. Окремим небажаним заходам можна запобігти, встановивши відповідні налаштування, інші варто брати до уваги. Встановлення будь-яких додатків на смартфон вимагає ретельного вивчення користувацьких угод, переліку опцій, процесів, дозволів, які програма запитує при інсталяції, для запобігання витоку персональної інформації до непорядних компаній. Недосвідченому користувачеві слід уникати або виявляти пильність, користуючись платними сервісами, які надають різні інтернет-ресурси. Нерідкими є факти зараження шкідливими програмами, крадіжки особистих та корпоративних даних, що відбуваються в результаті атак на мобільні пристрої.

Потенційні вразливості в пристроях інтернету речей дозволяють зловмисникам отримати доступ до мережі маршрутизатора, тим самим забезпечуючи собі шлях до інших об'єктів. Щоб запо-

бігти небезпеці, крім практики створення окремих та віртуальних мереж слід застосовувати і інші важливі принципи захисту, серед яких зміна заводських налаштувань пристрою з паролем по замовчанню, обов'язкове використання максимально довгих і унікальних паролей для усіх пристроїв системи. Оскільки велика кількість підключених елементів зв'язана з мобільними додатками, які при цьому можуть працювати у фоновому режимі та використовувати небезпечні дозволи, такі дозволи потребують коригування. Отже, кожна з технологій потребує ретельного вивчення та неухильного дотримання заходів інформаційної безпеки.

Однак не лише людина повинна турбуватися про власну захищеність. Свою відповідальність мають усвідомлювати і виробники нових технологій, програм, цифрових сервісів та ресурсів. Грамотні та продумані рішення мають зосереджуватися як на забезпеченні надійного захисту від зовнішніх загроз, так і на заходах, що здатні убезпечити людину при користуванні системами і продуктами від дій (випадкових, необережних чи пов'язаних з необізнаністю), які можуть стати причиною заподіяння шкоди їй або її майну.

Застарівання знань внаслідок швидких технологічних змін (поява та розповсюдження нових пристроїв, технологій, інтерфейсів) викликає потребу регулярно розширяти перелік цифрових навичок, набувати нових актуальних цифрових компетенцій, які відповідають вимогам середовища, у все зростаючій мірі. Це означає, що навчання має бути безперервним, користувачі мають розуміти важливість та бути готовими до постійного процесу засвоєння як особливостей застосування нових цифрових інструментів, так і вивчення та дотримання заходів безпеки при роботі з ними.

Величезну роль у набутті нових цифрових компетенцій має самоосвіта. Існує багато можливостей для придбання знань і розвитку навичок протягом життя. Навчання повинно відбуватися неминуче і постійно, добровільно і самовмотивовано. Проте частина населення не готова докладати істотних зусиль, щоб здійснювати оновлення низки актуальних навичок, мотивація окремих аудиторій людей до освоєння специфічних цифрових умінь є досить низькою. Отже, викликом часу є створення сприятливого середовища для безперервного навчання, актуального в умовах невідомості змін.

Турбуючись про прогресивний розвиток країни та своїх громадян, державні та приватні освітні організації, представники бізнесу, галузеві групи, професійні спільноти повинні бути зацікавлені у побудові адаптивної освітньої екосистеми, що швидко відповідає на зміни середовища, та створенні умов для реалізації загальних, орієнтованих на певні групи і персоналізованих траєкторій навчання. При цьому варто звернути увагу на той факт, що хоча молодь суттєво перевершує більш старші покоління з точки зору загального рівня володіння цифровими навичками і обізнаності щодо технологічних інновацій, значна частина зусиль в сфері розвитку цифрових компетенцій спрямована саме на осіб молодого віку, в той час як категорії, що потребують і знань, і мотивації, і впевненості, залишаються без адекватної підтримки. Зауваження не стосується дітей та юнаків, адже необхідність посиленого навчання цифровим компетенціям цієї групи обґрунтована важливістю забезпечення інформаційної захищеності юного покоління, що має на меті запобігання ризикам шкідливого впливу на їх здоров'я, розвиток і свідомість, мінімізацію загроз та відгуку на маніпуляції, реалізацію потреб у просвітництві та навчанні навикам аналізу і оцінки інформації, правилам поведінки в мережі, безпечному і розумному використанню інтернет-можливостей тощо, враховуючи вік, недостатній життєвий досвід і обсяг набутих знань.

В цілому свідомість користувачів і споживачів стосовно актуальних і потенційних загроз в цифровому середовищі зростає, отже росте потреба у постійному оновленні відповідних освітніх курсів і програм, а також в підтримці кваліфікації, вчасному освоєнні нових технологій та отриманні актуальних знань викладачами в умовах стрімких змін.

Підтримуючи курс на масштабну цифровізацію, наразі держава активно розробляє та пропонує широкому загалу для використання в житті і роботі національні цифрові продукти: онлайн-сервіси, портали онлайн-послуг, мобільні застосунки, електронні реєстри тощо. Оскільки разом з доступністю інформації підвищилась і її вразливість, на публічних структурах лежить велика відповідальність: забезпечити високу надійність та повний спектр заходів інформаційної безпеки для того, щоб дані кожного користувача чи

персони, конфіденційні відомості щодо якої містяться у ресурсах, були убезпечені від шкідливого впливу, крадіжки або несанкціонованого використання. Також при реалізації продуктів важливим є розуміння рівня звичайної людини, яка буде їх використовувати, з метою запобігання ситуаціям, що можуть поставити інформаційну безпеку під загрозу. Для цього відповідальні мають володіти спеціалізованими професійними цифровими компетенціями і навиками найвищого рівня. Ці цифрові навички мають забезпечувати регулярне вирішення складних технологічних завдань, чітке розуміння особливостей, актуальних тенденцій та ключових напрямків розвитку цифрового середовища та вміння їх реалізувати належним чином з дотриманням всіх норм інформаційної безпеки.

Інформаційна захищеність потреб особи в інформації, які супроводжують її існування, діяльність і прогресивний розвиток, не піддаючись негативному впливу внутрішніх і зовнішніх інформаційних загроз, напряду залежить від цифрової грамотності. На відповідних компетенціях засновується обґрунтованість рішень і дій, які здійснюються під час взаємодії з цифровим середовищем, що у підсумку забезпечує захист життєво важливих інтересів, прав та свобод людини.

Список використаної літератури:

1. Майже 23 млн українців регулярно користуються Інтернетом – дослідження [Електронний ресурс]. – Режим доступу: <https://mind.ua/news/20204323-majzhe-23-mln-ukrayinciv-regulyarno-koristuyutsya-internetom-doslidzhennya>
2. Обучение цифровым навыкам: глобальные вызовы и передовые практики. Аналитический отчет. / [авт. кол. Катькало В.С., Волков Д.Л., Баранов И.Н., Зубцов Д.А., Липчанский А.В., Соболев Е.В., Юрченков В.И., Старовойтов А.А., Сафронов П.А.]. – М.: АНО ДПО «Корпоративный университет Сбербанка», 2018.
3. European Union – “DigComp 2.1: The Digital Competence Framework for Citizens with eight proficiency levels and examples of use”, 2017.

Чинник П.А.,

студент 3-го курсу ІПСА КПІ ім. Ігоря Сікорського

Науковий керівник:

викладач кафедри публічного права

КПІ ім. Ігоря Сікорського

Іщенко В.В.

ПРАВО НА ІНФОРМАЦІЙНУ ПРИВАТНІСТЬ

З моменту появи у 1981 р. персонального комп'ютера захист інформаційної приватності та персональних даних потребує нових законів і їх постійного вдосконалення, тому що інформаційні технології не стоять на місці, а дуже великими темпами розвиваються весь час.

Приватність – це одна із фундаментальних прав людини, які визнані у всьому світі, а саме ст. 12 Загальної декларації прав людини ООН [1], та ст. 2 Міжнародного пакту про громадянські та політичні права [2]. Приватність тісно пов'язана з людською гідністю, свободою слова, свобода асоціацій тощо.

Інформаційна приватність – це приватність, що включає в себе встановлення правил збору та обігу персональних даних, таких як інформація кредитних установ та медичні записи [3].

Зростання інтересу до приватності почалося 60-70 рр. XX ст. з появою більш компактних комп'ютерів і автоматизованих систем. Із-за цього з'явилися потенційні можливості для стеження з допомогою потужних комп'ютерних систем. Тому треба було ставити на перший план вимоги встановлення спеціальних правил щодо збору та обігу інформації особистого характеру. У цій сфері першим законодавчим документом у світі був закон про захист даних, який було введено в дію на землі Гессен в Німеччині в 1970 р.

На міжнародному рівні було прийнято два надзвичайно важливих документи, які почали регулювати інформаційну приватність: Конвенція Ради Європи про захист осіб у зв'язку з обробкою інформації про особу та відсутністю обмежень на переміщення такої інформації Конвенція про захист осіб у зв'язку з автоматизованою

обробкою персональних даних від 28 січня 1981 р. [4] та Правила забезпечення захисту приватності у зв'язку із транскордонним переміщенням інформації про особу, встановлені Організацією Економічного Співробітництва та Розвитку (ОЕСР) від 24 жовтня 1995 р. [5], якими визначено спеціальні вимоги стосовно обігу електронних даних.

Також важливу роль відіграє Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) (англ. General Data Protection Regulation, GDPR) [6], що набрав чинності 25.05.2018 р. Це нормативний акт детально визначає фактичну сферу його застосування, територіальну дію, основні принципи, пов'язані з обробкою персональних даних, його мету, термін набрання чинності тощо. Регламент є обов'язковим у повному обсязі та підлягає прямому застосуванню у державах-членах ЄС.

Забезпечення конфіденційності персональних даних регулюють Конституція України, Закони України "Про захист персональних даних", "Про інформацію", рішення Конституційного суду України тощо. В Україні основну роль у формуванні механізму правового захисту персональних даних людини й громадянина розкривається через конституційні засади що містяться у ст. 3, 28, 30, 31, 32, 34, 35, 41, 54, 55, 64 Конституції України та нормативно-правових актах Європейського Союзу. Відсутність у тексті Конституції України спеціально визначеного права на захист персональних даних не є перешкодою для визнання цього права предметом конституційного захисту, оскільки такий захист передбачений комплексом положень конституційних норм розділу 2 Основного закону [7]. Відповідно до рішень Конституційного суду України у справі Устименка К.Г. від 30.10.1997 р. №5-зп та у справі щодо офіційного тлумачення ст. 3, 23, 31, 47, 48 Закону України «Про інформацію» та Рішення КСУ за конституційним поданням Жашківської районної ради щодо тлумачення ст. 32 Конституції України від 20 січня 2012 року № 2-рп/2012: «...забороняється не лише збирання, але й зберігання, використання та поширення конфіденційної інформації про особу

без її попередньої згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту, прав та свобод людини» [9; 10].

Основним актом, який регулює правила поводження з персональними даними є Закон України “Про захист персональних даних”, згідно зі ст. 2 якого: «персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Але таке визначення не досконале тим, що в ньому на концептуальному рівні відсутні критерії, за якими можна відрізнити персональні дані від будь-якої іншої інформації (наприклад, конфіденційної інформації про особу)» [8].

Таким чином, Україні потрібно своє законодавство приводити у відповідність до норм законодавства Європейського Союзу, оскільки останнє більш чітко врегульовує процедуру зберігання і доступ до персональних даних людини. Також потрібно дати більш чітке визначення персональних даних в Законі України “Про захист персональних даних”. На нашу думку, в Україні є необхідність у прийнятті окремого закону, який би регулював приватність людини в Інтернеті, щоб компанії не зловживали даними і не заробляли гроші на цьому без дозволу користувача.

Список використаних джерел:

1. Загальна декларація прав людини від 10 грудня 1948 року. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 18.05.2020)
2. Міжнародний пакт про громадянські і політичні права від 19 жовтня 1973 року. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 18.05.2020)
3. Доповідь “Приватність і права людини”, Девід Банісар (Electronic Privacy Information Center) та Саймон Девіс (Privacy International)
4. URL: <http://library.khpg.org/index.php?id=928437562> (дата звернення: 18.05.2020)
5. Конвенція про захист осіб у зв’язку з автоматизованою обробкою персональних даних URL: https://zakon.rada.gov.ua/laws/show/994_326 від 28 січня 1981 року (Дата звернення: 18.05.2020)

6. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046> (Last accessed: 18.05.2020)

7. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних). URL: https://zakon.rada.gov.ua/laws/show/984_008-16 (дата звернення 18.05.2020)

8. Головченко В. Правові основи захисту персональних даних. Юридича газета. Дата 05 вересня 2018, № 36 (638) URL: <https://yur-gazeta.com/publications/practice/inshe/pravovi-osnovi-zahistu-personalnih-danih.html> (дата звернення: 18.05.2020)

9. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17> (дата звернення: 18.05.2020)

10. Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України „Про інформацію” та статті 12 Закону України „Про прокуратуру” від 30 жовтня 1997 року № 18/203-97 .URL: <https://zakon.rada.gov.ua/laws/show/v005p710-97> (дата звернення: 18.05.2020)

11. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо тлумачення ст. 23 Конституції України від 20 січня 2012 року № 2-рп/2012 .URL: <https://zakon.rada.gov.ua/laws/show/v002p710-12> (дата звернення: 18.05.2020)

Якубовська Я.В.

здобувач СВО магістра Вінницький
державний педагогічний університет
ім.М.Коцюбинського

ОСОБЛИВОСТІ ЗАБЕЗПЕЧЕННЯ ПРАВ І СВОБОД ЛЮДИНИ В ІНФОРМАЦІЙНІЙ СФЕРІ В УМОВАХ ДЕЦЕНТРАЛІЗАЦІЇ ВЛАДИ В УКРАЇНІ

Права і свободи людини та гарантії їх забезпечення визначають зміст і спрямованість діяльності держави. Одним з напрямів державного та регіонального управління є децентралізація влади та формування нових відносин між центральними органами управління держави та новоутвореними органами територіального управління. В сучасних умовах, коли частина державних повноважень передається на місцевий рівень управління, особливості забезпечення прав і свобод людини також трансформуються.

Питання інформаційної безпеки в контексті державного управління та місцевого самоврядування висвітлювали у своїх працях фахівці в галузі державного управління: В. Б. Авер'янов, О. А. Баранов, В. І. Гурковський, Є. В. Жуков, Л. П. Коваленко, В. А. Ліпкан, І. В. Мукомела, О. В. Рибальський, І. М. Сопілко, В. В. Ткаченко.

Зважаючи на той факт, що в Україні на законодавчому рівні відсутня уніфікована дефініція категорії інформаційних прав, тому, використовуючи доктринальні напрацювання, варто акцентувати увагу на тому, що інформаційні права людини – гарантовані державою можливості людини задовольняти її потреби в отриманні, використанні, поширенні, охороні і захисті необхідного для життєдіяльності обсягу інформації [4].

Інформаційні права та свободи громадян знаходяться в органічному зв'язку з обов'язками держави в інформаційній сфері. Водночас Конституція України встановлює ряд принципових положень, що стосуються гарантій інформаційної безпеки: 1. Права і свободи людини і громадянина захищаються судом (ст. 55). 2. Кожен має право на повагу до його гідності (ч. 1 ст. 21). 3. Кожен має право на таємницю листування, телефонних переговорів, поштових, те-

леграфних та інших повідомлень. Обмеження цього права допускається лише на підставі судового рішення (ст. 31). 4. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом. (ч. 1 ст. 32). 5. Органи державної влади та органи місцевого самоврядування, установи і організації їх посадові особи зобов'язані забезпечити кожному можливість ознайомлення з документами і матеріалами, що безпосередньо зачіпають його права і свободи, відомостями про себе, якщо інше не передбачено законом (ч. 2 ст. 32). 6. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації (ч. 3 ст. 32). 7. Інтелектуальна власність охороняється законом (ст. 54). 8. В умовах воєнного та надзвичайного стану для забезпечення безпеки громадян і захисту конституційного ладу відповідно до конституційним законом можуть встановлюватися окремі обмеження прав і свобод із зазначенням терміну їх дії (ст. 64) [3].

Конституційне право на свободу отримання інформації є не тільки основою інформаційних відносин, а й гарантом прозорості та законності діяльності державної влади та місцевого самоврядування. Відповідно до Законів України «Про доступ до публічної інформації», «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних» до основних принципів забезпечення доступу до інформації про діяльність державних органів і органів місцевого самоврядування належать: відкритість і доступність інформації про діяльність державних органів та органів місцевого самоврядування; достовірність інформації про діяльність державних органів і органів місцевого самоврядування та своєчасність її надання; свобода пошуку, отримання, передачі та поширення інформації про діяльність державних органів і органів місцевого самоврядування будь-яким законним способом; дотримання прав громадян на недоторканність приватного життя, особисту і сімейну таємницю, захист їх честі і

ділової репутації, права організацій на захист їх ділової репутації при наданні інформації про діяльність державних органів і органів місцевого самоврядування [1, 2].

Взаємодія та підтримка зворотного зв'язку громадян з державними органами слід вважати невід'ємною ланкою права на доступ до інформації. За рівнями соціальної організації і геополітичним змістом інформаційна безпека може забезпечуватися на міждержавному, загальнодержавному та внутрішньодержавному рівні (на рівні регіональних інститутів), а також на рівні органів місцевого самоврядування.

У даний час спостерігається трансформація ролі держави, яка розширює свою участь у суспільних зв'язках як організатор залучаючи органи місцевого самоврядування та інститути громадянського суспільства. У випадках коли існують і розвиваються інноваційні механізми обміну інформацією та взаємодії між різними суб'єктами у сфері безпеки, це дасть можливість розвиватись сталому і безпечному середовищу в громадах. Також важливою умовою є інтеграція різних соціальних груп у життя громади, яке будуватиметься на засадах рівності, недискримінації та поваги до прав людини.

На рівні територіальної громади в межах місцевого самоврядування, завдяки компетенційним повноваженням органів місцевого самоврядування, що скеровані на вирішення питань місцевого значення, тобто питань від розуміння, визначення та вирішення яких залежить стабільне існування та функціонування територіальної громади та кожного з її членів – жителів відповідної території, – формується локальна система реалізації, охорони, захисту та гарантування конституційних прав, свобод і обов'язків людини і громадянина, що на локальному рівні функціонування соціуму виступають як муніципальні права людини, особистості, члена територіальної громади.

Конституція України встановлює, що усі мають право направляти індивідуальні чи колективні письмові звернення або особисто звертатися до органів державної влади, органів місцевого самоврядування та посадових і службових осіб цих органів, що зобов'язані розглянути звернення і дати обґрунтовану відповідь у встановлений законом строк. Дану конституційну норму мож-

на вважати гарантією та передумовою громадського контролю за органами державної влади, місцевого самоврядування та громадськими недержавними структурами, що передбачає рівний доступ до державних інформаційних ресурсів, за винятком інформації, що відноситься до державної таємниці [3].

Політика забезпечення інформаційної безпеки – це діяльність політичного керівництва країни з визначення цілей і постановки принципових завдань по захисту життєво важливих інтересів особи, суспільства та держави у інформаційній сфері та вироблення форм, методів і способів досягнення цих цілей [6].

Кожне повноваження органів місцевого самоврядування, що є зафіксованим на конституційному або на законодавчому рівні, в широкому його розумінні, є скерованим на виконання, охорону, захист та гарантування прав людини, що мешкає на відповідній території держави в рамках територіальної громади та в умовах місцевого самоврядування.

Політика забезпечення інформаційної безпеки здійснюється на принципах дотримання та захисту прав і свобод людини та громадянина, законності, дотримання балансу інтересів особи, суспільства та держави, взаємної відповідальності особи, суспільства та держави за підтримання належного рівня функціонування механізму забезпечення інформаційної безпеки; системності та комплексності застосування органами державної влади, органами місцевого самоврядування політичних, організаційних, соціально-економічних, інформаційних, правових і інших заходів забезпечення інформаційної безпеки; пріоритет попереджувальних заходів з метою забезпечення безпеки; взаємодія органів державної влади з громадськими об'єднаннями, міжнародними організаціями та громадянами з метою забезпечення інформаційної безпеки.

Адміністративно-правове забезпечення інформаційної безпеки полягає в виконавчо-розпорядчій діяльності органів державної влади та місцевого самоврядування з забезпечення виконання загальнообов'язкових умов та вимог безпеки, що пов'язано з безпосереднім втручанням в адміністративно-господарську, організаційно-розпорядчу і іншу діяльність фізичних і юридичних осіб, організаційно не підлеглих даними органам, врегульованою

нормами адміністративного права, здійснювана в цілях охорони та захисту законних інтересів учасників відносин, що виникають у сфері забезпечення інформаційної безпеки. Виконавча влада і адміністрація грають ключову роль в забезпеченні ефективного правління, але в умовах децентралізації частина повноважень щодо адміністративно-правового забезпечення покладена і на місцеве самоврядування. У самоврядних інститутів є свої власні функції, при виконанні яких вони не підзвітні виконавчій владі.

Політичні засоби забезпечення інформаційної безпеки утворюються сукупністю інструментів політичної боротьби, в якій беруть участь політичні сили суспільства: страйки, пропагандистські кампанії, критика політичних опонентів, мітинги, демонстрації, вибори, референдуми тощо.

Засоби технологічного забезпечення інформаційної безпеки - це сукупність технічних і програмних засобів захисту інформації, запобігання несанкціонованому доступу до інформаційних, телекомунікаційних та обчислювальних систем і мереж зв'язку, а також методичного забезпечення їх використання [5].

Протидія загрозам конституційним правам і свободам людини та громадянина у сфері духовного життя та інформаційної діяльності здійснюється з переважним використанням методів примусу. Умови для протидії утискам конституційних прав громадян на особисту та сімейну таємницю, таємницю листування, телефонних переговорів та інших повідомлень створюють норми Кримінального кодексу України, що закріплюють кримінальну відповідальність за порушення цих конституційних прав і свобод.

Для забезпечення безпеки функціонують правоохоронні органи. В умовах децентралізації, коли органи місцевого самоврядування можуть активно залучати громадськість до процесу управління постає можливість, щодо включення громадськості до забезпечення взаємодії з органами правопорядку. Важливим аспектом діяльності поліції є те, що вона реалізує спільні ініціативи з громадськістю. Поліція взаємодіє з громадськістю шляхом підготовки та виконання спільних проєктів, програм і заходів для задоволення потреб населення та покращення ефективності виконання поліцією покладених на неї завдань. Орган місцевого самоврядування

може бути ініціатором та організатором залучення населення до спільної розробки та реалізації ініціатив у сфері безпеки [7].

Таким чином, забезпечення інформаційної безпеки людини є складним комплексним поняттям, що охоплює велике коло процесів і явищ, пов'язаних із протидією загрозам безпеці особистих прав в інформаційній сфері.

Список використаної літератури

1. Закон України «Про внесення змін до деяких законів України щодо доступу до публічної інформації у формі відкритих даних»: редакція від 01.08.2016р. № 319-VIII [Електронний ресурс] // Відомості Верховної Ради України: – Текст. дані. – Київ 2016. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/319-19>

2. Закон України «Про доступ до публічної інформації»: редакція від 01.12.2019р. № 2939-VI [Електронний ресурс] // Відомості Верховної Ради України: – Текст. дані. – Київ 2019. – Режим доступу : <https://zakon.rada.gov.ua/laws/show/2939-17>

3. Конституція України: редакція від 01.01.2020 № 254к/96-ВР [Електронний ресурс] // Відомості Верховної Ради України: – Текст. дані. – Київ 2020. – Режим доступу: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80>

4. Куц І. Визначення поняття «інформаційні права людини» [Електронний ресурс] // І. Куц. – Режим доступу: <http://naub.ua.edu.ua/2012/vyznachennya-ponyattya-informatsijni-prava-lyudyny/>

5. Опанасенко Я. О. Роль і місце організаційної, соціальної й інформаційної складових у реалізації державної регіональної політики в умовах невизначеності регіонів / А. Л. Помаза-Пономаренко, Р. Т. Лукиша, Я. О. Опанасенко // Вісник Національного університету цивільного захисту України (Серія: Державне управління), 2016. – № 1 (4). – С. 203–209.

6. Почепцов Г. Інформаційна політика : навч. посіб. / Г. Почепцов, С. Чукут. – К. : Вид-во УАДУ, 2002. – 88 с.

7. Система публічного управління в умовах децентралізації влади: механізми горизонтальної взаємодії: монографія // Л.Л. Приходченко, С.Є. Саханенко, П.І. Надолішній та ін. ; за заг. ред. Л.Л. Приходченко. – Одеса : ОРІДУ НАДУ, 2017. – 135-160 с.

Наукове видання

**ЗАХИСТ ПРАВ, СВОБОД І БЕЗПЕКИ ЛЮДИНИ
В ІНФОРМАЦІЙНІЙ СФЕРІ В СУЧАСНИХ УМОВАХ**

МАТЕРІАЛИ
ДРУГОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

21 травня 2020 року

Формат 60*84/8
Папір книжково-журнальний 65гр/м2. Друк цифровий.
Гарнітура Minion Pro
Ум. друк. арк. 22,3 Обл.-вид. арк. 17,7.
Наклад 50 прим.

ТОВ «Видавничий дім «АртЕк»
04050, м. Київ, вул. Ю. Ільєнка, буд. 63
Тел.. 067 440 11 37
ph-artek@ukr.net
www.book-on-demand.com.ua

Свідоцтво про внесення суб'єкта видавничої справи
ДК №4779 від 15.10.14р.